Universidade Federal do Rio de Janeiro

Núcleo de Computação Eletrônica

Luiz Antônio Reis Silva

PROPOSTA DE METODOLOGIA PARA O EMPREGO OTIMIZADO DA REDUNDÂNCIA EM BUSCA DA ALTA DISPONIBILIDADE E DA MÁXIMA CONFIABILIDADE EM REDES.

Rio de Janeiro – RJ

2007

LUIZ ANTÔNIO REIS SILVA

PROPOSTA DE METODOLOGIA PARA O EMPREGO OTIMIZADO DA REDUNDÂNCIA EM BUSCA DA ALTA DISPONIBILIDADE E DA MÁXIMA CONFIABILIDADE EM REDES.

Monografia apresentada para obtenção do título de especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE / UFRJ .

Orientador :

Prof. Moacyr H. Cruz de Azevedo, M.Sc.,UFRJ, Brasil

Rio de Janeiro – RJ

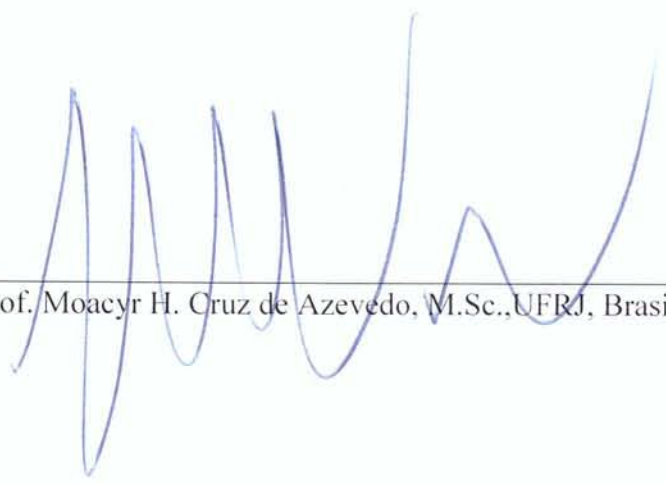
2007

LUIZ ANTÔNIO REIS SILVA

PROPOSTA DE METODOLOGIA PARA O EMPREGO OTIMIZADO DA REDUNDÂNCIA EM BUSCA DA ALTA DISPONIBILIDADE E DA MÁXIMA CONFIABILIDADE EM REDES.

Monografia apresentada para obtenção do título de especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE / UFRJ .

Aprovada em dezembro de 2007.



Prof. Moacyr H. Cruz de Azevedo, M.Sc., UFRJ, Brasil

Apesar de simples, mas por ter exigido um valoroso esforço, dedico este trabalho à Deus por permitir que pessoas próximas permanecessem mais próximas e que outras pessoas não tão próximas se aproximassem e, da mesma forma, contribuíssem com um voluntário e bem vindo apoio.

AGRADECIMENTOS

Agradeço a DEUS por ter a quem agradecer e por ainda poder abraçar a quase todos.
Agradeço aos meus pais por mostrarem o caminho e ainda retirarem pesadas pedras.
Agradeço a minha esposa e filha por serem o colírio do espírito no regresso tardio.
Agradeço as minhas irmãs e sobrinhos por mostrarem na luta, momentos de paz.
Agradeço a professores e todos os amigos de profissão pela parceria no calor da batalha.
Agradeço ao Comando do Material de Fuzileiros Navais pela oportunidade e pelas "armas".
Agradeço à MARINHA DO BRASIL por saber separar os Homens dos meninos maiores.
Agradeço ao BRASIL por ser o meu País e pela coragem de insistir em dar certo, como eu.

“Melhor Tratamento aos Pacientes com Sistemas mais Seguros.

O InCor tem uma rede com total redundância, sem um ponto de falha. "Nossos dois switches 3Com 4007 estão operando 24 x 7, se um deles tiver qualquer falha o outro continua em operação," descreve Gutierrez. "Nós precisamos da rede o tempo todo no ar porque monitoramos os sinais vitais dos pacientes. A segurança de nossos pacientes é nossa maior prioridade e nossa rede nos suporta com a disponibilidade das informações todo o tempo." ”

Informa Marco Gutierrez, Diretor Técnico do InCor.
Nome: HOSPITAL InCor — Instituto do Coração.
Localização: São Paulo, Brasil.
Nº de funcionários/pontos de rede: 2.500/1.500.
Nº de sites: 2.
Segmento de Mercado: Saúde.
http://lat.3com.c0om/br/casestudies/incor.html.

RESUMO

SILVA, Luiz Antônio Reis. **PROPOSTA DE METODOLOGIA PARA O EMPREGO OTIMIZADO DA REDUNDÂNCIA EM BUSCA DA ALTA DISPONIBILIDADE E DA MÁXIMA CONFIABILIDADE EM REDES.** Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2007.

Este trabalho se propõe a apresentar a necessidade de se obter um alto nível de disponibilidade e de confiabilidade dos serviços oferecidos por uma rede local e como alcançar este objetivo através do recurso da redundância. Com este intuito, é exposta a orientação técnica para a elaboração de uma ferramenta de apoio ao emprego da redundância chamada Planilha de Prioridades de SPOF (*Single Point of Failure)* (PPS). A proposta é utilizar a PPS para consulta e apoio à decisão de onde, como e a que custo aplicar, de forma racionalizada, o recurso da redundância e assim contribuir para mitigar os prejuízos que os citados SPOF podem produzir. Neste sentido, são levantados para cada SPOF identificado: os Riscos que a falha do SPOF representam; a respectiva Prioridade na eliminação; a Disponibilidade do componente (SPOF), de acordo com os princípios de MTBF (Mean Time Between Failures) e MTTR (Mean Time To Recover); e as Linhas de Ação, que são as alternativas de emprego do recurso da redundância de forma a reduzir ou eliminar os Riscos. As Linhas de Ação, preferencialmente, serão simuladas e testadas, das mais simples às mais complexas, de forma que seus resultados possam ser avaliados, registrados na PPS e os Custos estimados. Inicialmente, no Referencial Teórico, são mencionados alguns conceitos e definições, cuja compreensão é de relevante interesse para o acompanhamento do raciocínio aplicado. Considerando a oportunidade e a atualidade do assunto, é demonstrado o relacionamento prático do tema central com o conceito de Qualidade de Serviço. Da mesma forma são expostas algumas importantes técnicas de aplicação do recurso da redundância, hoje encontradas no mercado. Na Metodologia de Pesquisa são definidas as fases a serem cumpridas para se montar a PPS. Posteriormente, na Descrição de Caso, é descrito um modelo de instalação que será avaliado no capítulo seguinte, a fim de elaborar a PPS. Assim, é apreciada a possibilidade de, com a adequação do recurso da redundância às necessidades expostas na PPS, otimizar a busca por uma rede de dados mais disponível e confiável.

ABSTRACT

SILVA, Luiz Antônio Reis. **PROPOSTA DE METODOLOGIA PARA O EMPREGO OTIMIZADO DA REDUNDÂNCIA EM BUSCA DA ALTA DISPONIBILIDADE E DA MÁXIMA CONFIABILIDADE EM REDES.** Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2007.

The purpose of this paper is to show the necessity of have a high level of availability and trustworthy in a local area network service and how to reach that aim using redundancy. At this way, is exposed a technical orientation that will permit to elaborate a support tool for the redundancy application called Planilha de Prioridades de SPOF (Single Point of Failure) - Table of SPOF Priority (PPS). The proposal is use the PPS for consultation and to support the decision making of where, how and how much is to rationally apply the redundancy resource and then contribute to moderate the negative results that can be provoked by SPOF. In PPS are defined, for each identified SPOF: the Risks that the failure of SPOF represents; the Priority of elimination; the Availability of the component, considering MTBF (Mean Time Between Failures) and MTTR (Mean Time To Recover); and the Action Lines that are alternatives to apply redundancy resource, in order to reduce risks or to eliminate then. The Action Lines will be preferentially simulated and tested, from the less complex to the most, in order to enable the valuation results, cost estimation and registration in the PPS. Initially, some important conceptions and definitions are mentioned in Theoretician Referential, because their comprehension is interesting to accompany the applied reasoning. Considering the opportunity, is demonstrate the practical relationship among the subject and QoS. Some important redundancy resource application technics, nowadays commercial used, are shown. In Research Methodology the phases to construct PPS are defined. After that, in Case Description, a model of network installation is described, this model will be evaluate in the next chapter, in order to elaborate the PPS. Therefore, is appreciate the possibility of, with appropriation of the redundancy resource to the PPS necessities, optimize the search of a maximum trustworthy and high availability network.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ARP	*Address Resolution Protocol*
CARP	*Common Address Redundancy Protocol*
DMZ	*Demilitarized Zone*
ET	Estação de Trabalho
EA	Exequível e Aceitável
FW	*firewall*
GLBP	*Gateway Load Balancing Protocol*
HA	*High Availability*
HDTV	*High Definition Television*
HSRP	*Hot Standby Router Protocol*
ICMP	*Gateway Load Balancing Protocol*
IETF	*Internet Engineering Task Force*
IP	*Internet Protocol*
IRDP	ICMP *Router Discovery Protocol*
LA	Linha de Ação
LAN	*Local Área Network*
MAC	*Media Access Control*
MB	*Mega Byte*
MTBF	*Medium Time Between Failures*
MTTR	*Medium Time To Recover*
OSPF	*Open Shortest Path First*
PPS	Planilha de Prioridades de SPOF
RAID	*Redundant Array of Inexpensive Disks*
RIP	*Routing Information Protocol*
RPS	*Redundant Power Supply*
SLA	*Service Level Agreement*
SLB	*Server Load Balancing*
SPOF	*Single Point Of Failure*
SRM	*Single Router Mode*
SSI	*Single System Image*
UPS	*Uninterruptable Power Supply*
UTP	*Unshielded Twisted Pair*
VDC	*Volts Direct Current*
VPN	*Virtual Private Netware*
VRRP	*Virtual Router Redundancy Protocol*
WAN	*Wide Área Network*

SUMÁRIO

1 **INTRODUÇÃO**

1.1 MOTIVAÇÃO

O avanço tecnológico hoje observado acaba por estabelecer definitivamente a dependência operacional e administrativa das instituições em relação à sua estrutura de redes de comunicação. Ao possuir a capacidade praticamente ilimitada de conexões e absorver funcionalidades como armazenagem de dados, suporte a tráfego de dados, áudio e vídeo de forma convergente, além de um conjunto diversificado de aplicações simultâneas, a rede deve atender a quesitos básicos como: desempenho, segurança, disponibilidade, confiabilidade, entre outros. Apesar de não se tratar de conceitos compartimentados, mas sim inter-relacionados, as propriedades "disponibilidade" e "confiabilidade" serão aqui tratadas de forma mais específica. Isto se deve ao fato de que, ao adotar o recurso da **redundância**, tema central desta monografia, procura-se principalmente agregar uma alta disponibilidade e máxima confiabilidade aos serviços prestados por uma LAN.

Origem: Wikipedia, http://pt.wikipedia.org. 20/06/07
"Redundância é o meio mais eficaz de obter-se um sistema de alta disponibilidade.
A redundância de interfaces de rede, de CPU, de servidores, de fontes de alimentação interna mantém o perfeito funcionamento do sistema mesmo em caso de falhas de componentes ou sobrecargas do sistema."

São apresentados os estudos que, pela forma diversificada de abordagem da aplicação da redundância, contribuíram de forma relevante para o desenvolvimento deste trabalho:

- GARANTIA DE DISPONIBILIDADE EM AMBIENTE PEER – TO - PEER UTILIZANDO REPLICAÇÃO COORDENADA.
  José Nogueira D´Almeida Júnior.
  Universidade Federal do Rio de Janeiro, COPPE – 2005.

- UM PROTOCOLO TOLERANTE A FALHAS PARA DISSEMINAÇÃO DE DADOS EM REDES DE SENSORES SEM FIO.
  Bruno Ávila Galvão.
  Universidade Federal do Rio de Janeiro, NCE – 2005.

- DETECÇÃO E DIAGNÓSTICO DE FALHAS EM ROBÔS MANIPULADORES VIA REDES NEURAIS ARTIFICIAIS.
  Renato Tinós.
  Universidade de São Paulo – SP – 1999.

- SOBREVIVÊNCIA EM REDES ÓPTICAS TRANSPARENTES.
  Marco Dias Dutra Bicudo.
  Universidade Federal do Rio de Janeiro, COPPE – 2005.

1.2 OBJETIVO

É evidente que a perfeita funcionalidade de uma LAN envolve a observação de requisitos diversos, como: *modularidade*[1]; *manutenibilidade*[2]; *escalabilidade*[3]; *disponibilidade*[4]*; desempenho*; *confiabilidade*[5] entre outros. Neste estudo, pretende-se demonstrar que a crescente exigência quanto à disponibilidade e à confiabilidade operacionais de uma estrutura de rede de comunicações podem ser alcançadas através da aplicação otimizada do recurso da redundância.

A confiabilidade original de componentes dos Sistemas de Informação pode ser relativamente insuficiente para um serviço crítico. Para garantir a ausência de interrupções de serviço muitas vezes é necessário dispor de recursos redundantes que entrem em funcionamento, automaticamente gerenciados pela previsibilidade lógica, quando da falha de um dos componentes em produção.

Nesta linha de raciocínio, fica naturalmente exposto o seguinte questionamento:

Como viabilizar o emprego otimizado da redundância de componentes críticos de uma rede local estruturada, de forma a obter alta disponibilidade e máxima confiabilidade dos serviços e recursos oferecidos pela mesma?

1.3 RELEVÂNCIA

O tema proposto é de relevante importância prática, uma vez que poderá estimular maior reflexão sobre a adoção de métodos, protocolos e plataformas físicas e lógicas que priorizem não apenas o estabelecimento de conexões em rede, mas também a adequada confiabilidade e disponibilidade da estrutura em questão.

Teoricamente, quanto maior a redundância aplicada, menos pontos de falha existirão e menor será a probabilidade de interrupções no serviço. Há poucos anos tais sistemas eram muito dispendiosos, a redundância necessária gerava gastos, impelindo uma intensa busca por soluções alternativas de menor custo. Houve a necessidade de abordagens e de pesquisas mais dedicadas. Então, começaram a surgir alternativas mais viáveis e tecnicamente evoluídas, como sistemas construídos com *hardware* acessível, altamente escaláveis e de custo mínimo.

---

[1] É o termo para uma rede que é composta de várias partes que podem ser trocadas, assim um sistema pode ser dividido em vários subsistemas;
[2] Atributo que caracteriza a facilidade de modificação ou adaptação de uma rede;
[3] Habilidade de manipular uma porção crescente de trabalho de forma uniforme, ou estar preparado para o crescimento do mesmo;
[4] Capacidade de estar disponível para uso;
[5] Probabilidade de um item desempenhar uma função, sob condições específicas, de forma confiável;

São cada vez mais comuns para as aplicações em rede o uso de termos como “24 x 7” e “24 x 7 x 365”, referindo-se às horas do dia, dias da semana e dias do ano em que os serviços devem permanecer disponibilizados. Assim, justifica-se uma avaliação mais detalhada da aplicação do recurso da redundância, que praticamente viabiliza a disponibilidade integral dos serviços confiáveis de uma LAN. Desta forma, propõe-se que seja considerado como fator condicionante e determinante para a aceitação de um projeto concluído, a previsão de disponibilidade e confiabilidade máximas dos serviços prestados pela rede.

Segundo Kurose (2001, apud ANDERSON KARING, 2002, p. 1), devido ao fato de uma rede de computadores consistir de muitas partes complexas de *hardware* e *software*, tais como *links*, equipamentos, pontes, roteadores e outros dispositivos, quando centenas ou milhares destes dispositivos são conectados uns aos outros para formar uma rede, é de se esperar que componentes irão eventualmente funcionar mal, que elementos de rede poderão ser desconfigurados, que recursos da rede serão superutilizados, ou que componentes de rede irão simplesmente “quebrar”.

O raciocínio acima exposto é de fato confirmado pelas restrições técnicas presentes na grande maioria das instalações hoje existentes. Porém, existem sedimentados investimentos em redundância da forma como é aqui apresentada, sendo um importante recurso utilizado na busca da adequação técnica da rede, nos atuais padrões de confiabilidade e disponibilidade exigidos.

1.4 CONTRIBUIÇÃO

Em resposta ao questionamento exposto no item 1.2 e em complemento das informações aqui constantes, pretende-se oferecer exemplos de aplicações em que a utilização da redundância colabora de forma determinante para a adequada operação da rede. A contribuição básica é, diante do quadro a ser exposto com exemplos de técnicas atualizadas, oferecer apoio a decisão de como, quando e onde aplicar o recurso da redundância.

Atualmente são encontrados diversos cenários que exercem certa “pressão” sobre a confiabilidade e a disponibilidade dos *backbones* dos provedores. Serviços críticos que envolvem operacionalização de hospitais, movimentações financeiras, automação industrial, entre outras aplicações em tempo real, exigem risco zero de inoperância.

É real a possibilidade lógica e física de aperfeiçoar a qualidade dos serviços prestados por uma rede através de adições, verificações e ajustes de redundância. Fatores diretamente

ligados a QoS como: Atraso Fim-a-Fim, Variação do Atraso (*Jitter*), Perda de Pacotes e Largura de Banda, podem ser positivamente influenciados. Entretanto, existem restrições para as instalações já existentes, pois a partir de um determinado ponto, que envolvem fatores relevantes principalmente como o custo, a complexidade de gerência e de manutenção do equipamento, em último caso, apenas um projeto completamente novo pode oferecer resultados satisfatórios.

2 REFERENCIAL TEÓRICO

A redundância é um tema extremamente amplo e com possibilidades de exploração ilimitadas. Pretende-se, neste estudo, manter o foco nos principais componentes físicos de uma LAN e na respectiva lógica empregada na implementação da **redundância** dos mesmos. Para haver um adequado acompanhamento do raciocínio aplicado no estudo em questão, alguns princípios básicos são externados neste capítulo.

2.1 DEFINIÇÃO BÁSICA DE LAN

Pode-se caracterizar uma rede local como sendo uma rede que permite a interconexão de equipamentos de comunicação de dados numa pequena região (SOARES 1995). São redes privadas contidas em um único edifício ou *campus* universitário com até alguns quilômetros de extensão (TANENBAUM-2003).

2.2 DEFINIÇÃO BÁSICA DE DISPONIBILIDADE

É a capacidade que um recurso possui de estar pronto para uso. Neste contexto, um sistema de ***alta disponibilidade*** (HA) será um sistema informático resistente a falhas de *software, hardware* e de energia, cujo objetivo é manter os serviços disponibilizados o maior de tempo possível.

Disponibilidade é uma palavra comum entre os fornecedores de serviço. Com o acompanhamento adequado é possível definir a disponibilidade de um recurso (*link, hardware*, serviço, etc.) e, a partir desta definição, passar a medir e compreender os resultados. Pode-se, então, planejar os investimentos, aferir multas contratuais, bem como compreender o atendimento prestado por uma equipe e assim promover ações de melhoria.

O Quadro 1 ilustra um dos termos de comparação geralmente utilizado na avaliação de soluções HA: níveis de disponibilidade, segundo os tempos de indisponibilidade (*downtime*). Foram excluídos deste quadro os tempos de *downtime* estimados usados para manutenção ou reconfiguração dos sistemas, que são alheios às soluções e muito variáveis.

Quadro 1 - Níveis de Alta Disponibilidade – Fonte www.wikipedia.org.br

Disponibilidade (%)	*Downtime*/ano	*Downtime*/mês
95%	18 dias 6:00:00	1 dia 12:00:00
96%	14 dias 14:24:00	1 dia 4:48:00
97%	10 dias 22:48:00	0 dia 21:36:00
98%	7 dias 7:12:00	0 dia 14:24:00
99%	3 dias 15:36:00	0 dia 7:12:00
99,9%	0 dia 8:45:35.99	0 dia 0:43:11.99
99,99%	0 dia 0:52:33.60	0 dia 0:04:19.20
99,999%	0 dia 0:05:15.36	0 dia 0:00:25.92

2.2.1 **Tempo Médio entre Falhas (MTBF)**

O *tempo médio entre falhas* é o intervalo médio de tempo, geralmente medido em horas, entre duas falhas consecutivas. Está relacionado com a confiabilidade de componentes e o nível de redundância aplicado. Para obter este tempo basta levantar todas as paradas do dispositivo que se pretende avaliar e, utilizando recursos de estatística, como uma média aritmética , aplicar os valores obtidos e assim terá o MTBF.

2.2.2 **Tempo Médio de Recuperação (MTTR)**

O *tempo médio de recuperação* é o tempo médio de recuperação de problemas que tenham tornado indisponível um serviço ou a rede como um todo. Pode ser diminuído com o auxílio de redundância, mecanismos de autoteste e diagnósticos preventivos, além de execução de uma manutenção eficiente. Independentemente da solução adotada, existe sempre um MTTR, também definido como o espaço de tempo (médio) que decorre entre a ocorrência do problema e a total recuperação do sistema ao seu estado operacional. Procedendo-se do mesmo modo para obter o MTBF, será obtido o MTTR.

2.2.3 **Avaliação da Disponibilidade**

Geralmente, quanto maior a exigência de disponibilidade, maior a necessidade de redundância e o custo das soluções, tudo depende do tipo de serviço que se pretende manter disponível. Por exemplo: um operador de telecomunicações exigirá o mais elevado nível de disponibilidade de seus serviços, sob pena de perder os seus clientes, no caso do sistema sofrer falhas constantes. No entanto, uma empresa com horário de trabalho normal poderá considerar que 90% de disponibilidade serão suficientes. Salienta-se que o nível de disponibilidade mensal é, naturalmente, menor que o anual, não considerando-se o valor médio, mas sim o absoluto. Efetivamente, para se obter um nível de disponibilidade mensal de 97%, significa que o serviço fica inativo 3% do tempo, ou seja, durante 21,6 horas das 720 horas de um mês. Esta mesma indisponibilidade de 21,6 horas, considerada no total de horas de um ano, ou seja, 8.640 horas, representaria 0.25% do tempo total inativo, assim, neste patamar o nível anual de disponibilidade seria de 99,75% [10].

A disponibilidade pode ser medida da seguinte forma:

Disponibilidade = ((MTBF) / (MTBF + MTTR)).100% onde:

MTBF (*Mean Time Between Failures)* é o tempo médio entre a ocorrência de falhas e MTTR (*Mean Time To Recover*) é o tempo médio de reparo.

Exemplificando : Se um servidor pára a cada 12 dias durante 02 horas em média, temos que:

MTBF = 12 x 24 = 288 horas; e MTTR = 2 horas; então :

Disponibilidade = ((288) / 288 + 2)) . 100% = 99,31 %.

Desta forma, os efeitos decorrentes da indisponibilidade podem ser estimados.

É importante ressaltar que quanto maior o índice de disponibilidade exigido, maiores serão os investimentos e consequentemente os custos envolvidos.

2.3 DEFINIÇÃO BÁSICA DE CONFIABILIDADE

É a probabilidade de um item desempenhar uma função, sob condições especificas, de forma confiável. O termo "confiabilidade" se traduz lexicograficamente como a qualidade ou o estado daquilo em que se pode confiar, que é justamente o que se pretende obter de uma rede de dados, nos atuais padrões de desenvolvimento tecnológico. Apesar de serem termos diferentes, a confiabilidade, assim como a disponibilidade, também pode ser avaliada através da observação e controle dos princípios técnicos como: MTBF e MTTR.

O básico para se compreender a grande diferença entre disponibilidade e confiabilidade é o fato de que não há como um serviço ser confiável se ele não estiver disponível. Ou seja, o primeiro quesito a ser cumprido para verificar se um serviço é confiável é que ele esteja disponível.

2.3.1 **Reconfiguração Após Falhas**

Reconfiguração após falhas é a propriedade que o sistema deve possuir de, durante o menor tempo de latência[6] possível, ser reconfigurado, automaticamente ou não, voltando a operar normalmente após o problema. Requer que caminhos redundantes sejam acionados tão logo ocorra a falha ou esta seja detectada. A rede deve ser tolerante a falhas transientes ou permanentes causadas por *hardware/software*, de forma que tais falhas causem apenas uma confusão momentânea, resolvida em algum nível de reiniciação. Falhas de alguns componentes críticos ou destruição de programas poderão não ser resolvidas sem recursos de redundância.

2.3.2 **Degradação Amena**

Degradação amena mede a capacidade da rede continuar operando na presença de falhas, embora com um desempenho menor. É geralmente dependente da aplicação.

2.3.3 **Tolerância a Falhas**

É a propriedade desejável de uma rede de comunicações que permite que a mesma permaneça operando adequadamente mesmo após falhas em alguns de seus componentes. Se sua qualidade de operação diminui, a queda é proporcional à severidade da falha. A

[6] É a diferença de tempo entre a percepção da necessidade de reconfiguração e o momento em que seus efeitos tornam-se perceptíveis;

tolerância a falhas é uma propriedade prioritária em sistemas de alta disponibilidade ou em aplicações críticas. Consiste, basicamente, em ter *hardware* redundante que entra em funcionamento automaticamente após a detecção de falha no *hardware* principal.

2.4 ACORDO DE NÍVEL DE SERVIÇO

Um **Acordo de Nível de Serviço** (**ANS** ou **SLA** (*Service Level Agreement*)) é a parte de contrato de serviços entre duas ou mais entidades no qual o nível da prestação de serviço é definido formalmente. Na prática, o termo é usado no contexto de tempo de entregas de um serviço ou de um desempenho específico. Por exemplo, se a Empresa 'A' contratar um nível de serviço de entregas de 95% em menos de 24 horas à Empresa 'B', esta terá que fazer no mínimo 95% de todas as entregas de sua incumbência, em menos de 24 horas. O SLA tem relação direta com a disponibilidade e a confiabilidade do serviço oferecido.

2.5 INFLUÊNCIA DA DISPONIBILIDADE E DA CONFIABILIDADE NOS QUESITOS DE QOS

Como forma de observar a influência técnica que a adequação às exigências de confiabilidade e disponibilidade de uma rede pode exercer na Qualidade de Serviço obtida, cabe aqui a menção do conceito de QoS e dos quesitos relacionados.

Qualidade de Serviço é, resumidamente, a capacidade da rede de prover um melhor serviço a tráfego selecionado, operando sobre diferentes tecnologias. Algo que pode-se medir e definir políticas. Os quesitos de QoS são monitorados de forma a fornecerem os parâmetros necessários para o devido acompanhamento do desempenho dos serviços da rede. Se a redundância é uma ferramenta utilizada para diminuir ou evitar interrupções dos serviços de rede, é previsível que esta colabore de forma significativa na obtenção de melhores índices de QoS na mesma rede. Neste sentido, abaixo são expostos os quesitos básicos de QoS.

2.5.1 **Atraso fim-a-fim**

Trata-se do tempo que um pacote precisa para transcorrer do seu ponto de origem até o ponto de destino. Se neste percurso os SPOF (*Single Point of Failure* – explicado no item 3.2.2) identificados receberem recursos redundantes de forma a minimizar o risco de falha, o tempo de transcurso do pacote será otimizado.

2.5.2 **Variação do Atraso (Jitter)**

Variação de atraso que poderá existir entre pares de pacotes que trafegam na rede. Trata-se da variação na cadência do tráfego de pacotes, extremamente prejudicial para áudio ou vídeo. Uma das formas de minimizar a variação de atraso é a utilização de *buffer*, que armazena os dados a medida que eles chegam e os encaminha para a aplicação a uma mesma

cadência. Uma rajada ou tráfego intenso poderá estourar *buffers*, causar perdas de pacotes e a consequente queda de QoS. Dentro do princípio da redundância, recursos lógicos como *spanning-tree* ou *links resilientes* (explicados nos itens 2.6.7 e 2.6.8) colaboram no sentido de evitar o *jitter*.

2.5.3 **Perda de Pacotes**

Perda de pacotes se dá quando um determinado pacote, por razões diversas, não atinge o seu destino corretamente. Aplicações como voz e vídeo são extremamente sensíveis à esta perda. Assim como foi tratada nos itens anteriores, a identificação e eliminação de SPOF minimizam a perda de pacotes e elevam a qualidade do serviço.

2.5.4 **Largura de Banda**

É a capacidade de transmissão de dados que um determinado meio possui. É a capacidade máxima de transmissão deste meio. Este quesito também pode ser positivamente influenciado, neste caso pelo recurso de *Load Balance,* explicado no item 2.6.3.1.2.

2.6 REDUNDÂNCIA - EM BUSCA DE ALTA DISPONIBILIDADE E DE MÁXIMA CONFIABILIDADE

Mesmo compreendido sob o enfoque técnico, o termo "redundância" não deixa de ser extremamente genérico e explorado em amplitudes variadas. Na busca por benefícios econômicos na área de redes, em relação às missões críticas de comunicações, a confiabilidade e a disponibilidade tornam-se cruciais. As atenções se concentram no sentido de prover uma estrutura que esteja disponível 100% do tempo. Disponibilidade e confiabilidade de rede são baseada em dois alicerces principais. O primeiro é eliminar qualquer SPOF, adicionando garantias operacionais pautadas basicamente em componentes redundantes, serviços de rede redundantes e conexões para múltiplos *links* de LAN. O segundo é distribuir inteligência pela arquitetura, através de equipamentos de conexão com capacidade de processamento e armazenamento adequados ao serviço. Com o projeto apropriado, nenhum SPOF impactará na disponibilidade do sistema.

A melhor prática é o projeto baseado em blocos hierárquicos modulares que podem ser replicados para um crescimento sustentável. A infra-estrutura deve ser capaz de detectar e responder rapidamente a qualquer possível falha de serviço. Usuários e aplicações não notarão falhas se tecnologias resilientes otimizadas possibilitarem a rápida convergência destas falhas. Para alcançar este nível de convergência, múltiplas tecnologias de rede precisam interoperar e serem complementares, deste modo será obtido como resultado uma pronta recuperação.

Para melhor especificar a sua utilização no universo das redes de dados, foram selecionados alguns exemplos práticos da aplicabilidade da redundância em aspectos diversificados.

2.6.1 **Redundant Array of Inexpensive Disks (RAID)**

A eliminação de SPOF, fator a ser perseguido em uma LAN, possui solução com o uso da redundância de recursos como: servidores, discos rígidos, placas de rede, roteadores, *switchs,* processadores, entre outros componentes. Os discos rígidos, que são alguns dos mais importantes componentes de *hardware* por armazenarem os dados corporativos, merecem especial atenção já que também são suscetíveis a falhas. A realização de *backup* é uma solução possível, apesar de não contribuir para a Alta Disponibilidade pois não aumenta diretamente o *uptime*[7]. Uma das técnicas realmente aplicadas para a eliminação de SPOF é a utilização de *hardware* redundante, como o RAID.

Trata-se de um conjunto redundante de discos baratos que são combinados para aumentar a *performance*. A um nível mais complexo, o RAID pode ser usado para melhorar a confiabilidade do equipamento por meio de espelhamento ou paridade. O principio básico dessa tecnologia é, através da combinação de uma matriz formada por discos "pequenos", gravar dados com redundância para prover tolerância a falhas, ou dividí-los para aumentar a performance.

2.6.1.1 Tipos de RAID

Existem vários níveis de RAID, sendo que os mais usualmente encontrados são: RAID 0, RAID 1, RAID 0+1 e RAID 5.

No RAID 0 (processo em que ocorre *data striping* – divisão de dados) os dados são divididos em pequenos segmentos e distribuídos para armazenamento simultâneo entre os discos disponíveis, proporcionando alta *performance* na gravação e na leitura de informações. Como não oferece redundância, não é tolerante a falhas.

No RAID 1 (processo em que ocorre *mirroring* – espelhamento de dados) os dados são gravados em 2 ou mais discos ao mesmo tempo, oferecendo redundância destes dados e fácil recuperação, com proteção contra falha em disco. Uma característica do RAID 1 é que a gravação de dados é mais lenta, pois é feita duas ou mais vezes. No entanto, a leitura é mais rápida, pois o sistema pode acessar duas fontes para a busca de informações.

No RAID 0+1 é feita uma combinação do RAID nível 0 e do RAID nível 1. Neste os dados são divididos entre dois discos e duplicados para os demais. Desta forma obtém-se

---

[7] Duração do intervalo de tempo em que uma máquina permanece em operação ininterruptamente;

uma combinação da *performance* do RAID 0 com a tolerância a falhas do RAID 1. Para a implantação do RAID 0+1 são necessários no mínimo 4 discos, o que torna o sistema mais oneroso.

No RAID 5 os dados são divididos (em blocos e não a nível de bytes) entre os discos. Como todos os bytes têm a sua paridade (acréscimo de 1 bit para identificação de erros) distribuída por todos os discos da matriz, ocorre uma gravação de dados mais rápida, porque não existe um disco separado do sistema que possa gerar um "gargalo". Porém, como a paridade tem que ser dividida entre os discos a performance é ligeiramente prejudicada. O RAID 5 é amplamente utilizado em Servidores de grandes corporações por oferecer boa performance e confiabilidade ideal para aplicações não muito pesadas. É possível assegurar a integridade dos dados para recuperações necessárias.

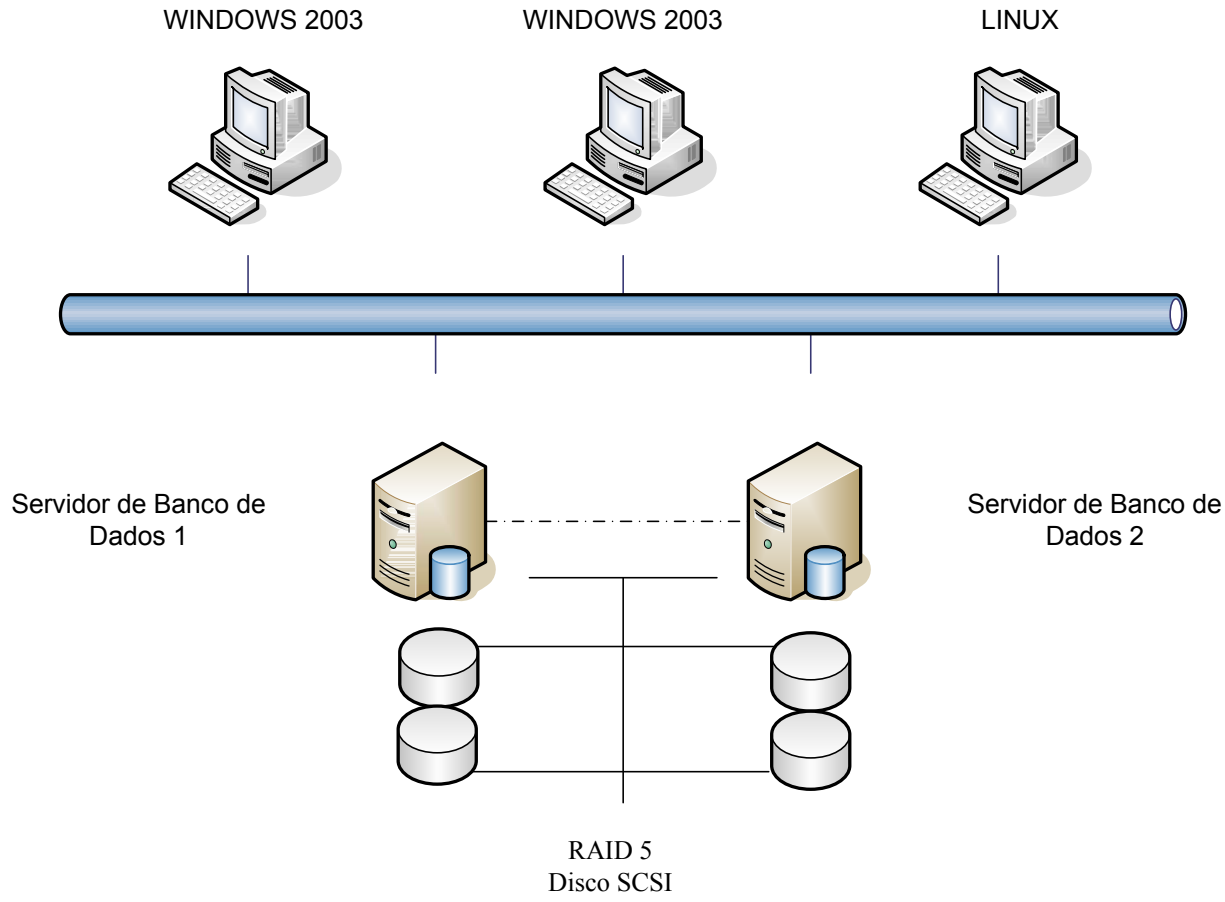


Figura 1 – Sistema de alta disponibilidade com redundância de servidores e RAID

2.6.2 **Balanceamento de Carga (Load Balance)**

Balanceamento efetuado pelos sistemas de processamento distribuído, que consiste em dividir a carga total de processamento pelos processadores disponíveis no sistema, sejam eles locais ou remotos. Considerando as limitações físicas impostas pelo *hardware*, em

termos de capacidade de armazenamento, processamento, transmissão, entre outras, muitas vezes um mesmo serviço deverá ser dividido entre componentes equivalentes, evitando sobrecargas, congestionamentos e retardos indesejados. O balanceamento de tráfego de uma rede, por exemplo, exige o encaminhamento de dados por caminhos alternativos a fim de descongestionar os acessos a pontos críticos como servidores.

A Figura 2 sugere a existência de um dispositivo responsável pelo balanceamento denominado balanceador ou *director*. Na verdade, ele pode existir sob várias formas, dependendo do serviço que se pretende balancear. Este balanceador serve também de interface entre o *cluster de servidores* (explicado a partir do item 2.6.3) e os clientes dos serviços. O recurso da redundância participa deste processo na medida em que, para que haja o efetivo balanceamento de um dado serviço, o provedor deste serviço deve possuir um determinado grau de redundância seja no nível de processamento, armazenamento, transmissão ou outro qualquer.

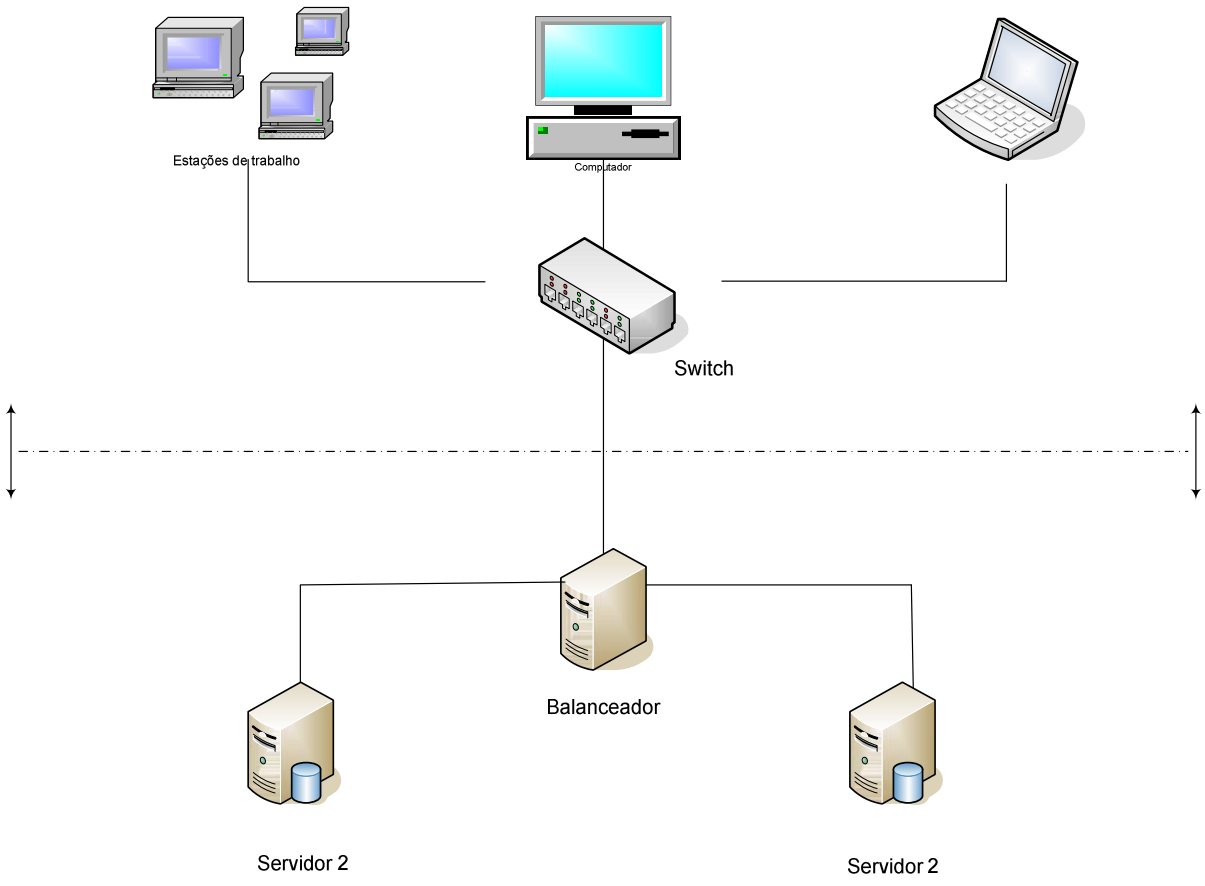


Figura 2 – Sistema de Balanceamento de Carga entre servidores via balanceador.

2.6.3 **Cluster**

Agrupamento de computadores que, interconectados por uma rede e trabalhando em conjunto, podem processar um volume maciço de dados, manter serviços disponíveis de forma praticamente ininterrupta e reduzir a sobrecarga de requisições no sistema. É visto pelo usuário como se fosse uma única máquina. Cada máquina do agrupamento, também chamado de aglomeração de computadores, recebe o nome de *nó* ou *nodo*. Esta técnica possibilita disponibilizar recursos para processamentos pesados, sem que haja o investimento em máquinas de alto custo, fazendo com que um conjunto de máquinas comuns possam executar tarefas de máquinas tecnologicamente complexas. Desta forma, passa a haver uma maior garantia de que os serviços estejam mais disponíveis e confiáveis. Resumidamente, *cluster* é uma importante técnica que permite que um grupo de computadores "modestos" dividam tarefas de processamento e trabalhem como um único computador de maior capacidade. Esta característica de transparência é conhecida como SSI[8] (*Single System Image*).

2.6.3.1 Tipos de Cluster

2.6.3.1.1 Alta Disponibilidade (High Availability (HA) and *Failover*)

Estes modelos de *clusters* são construídos para prover uma disponibilidade de serviços e recursos ininterrupta, através do uso da redundância implícita ao sistema. A idéia geral é que se um nó do *cluster* vier a falhar, aplicações ou serviços possam estar disponíveis em outro nó (*failover*[9]). Este tipo de *cluster* é utilizado para base de dados de missões críticas, correio, servidores de arquivos e aplicações.

2.6.3.1.2 Balanceamento de carga (Load Balance) em Cluster

Este modelo distribui o tráfego entrante ou requisições de recursos provenientes dos nodos que executam os mesmos programas, entre as máquinas que compõem o *cluster*. Todos os nodos estão responsáveis em controlar os pedidos. Se um nó falhar as requisições são redistribuídas entre os nós disponíveis no momento. Este tipo de solução é normalmente utilizado em fazendas de servidores *web* (*web farm*[10]). A intenção é manter vários

---

[8] Ilusão criada pelo *software* e/ou *hardware* que apresenta um conjunto de recursos de computação como sendo um recurso único.

[9] É a capacidade que possui um sistema de trocar automaticamente um dispositivo em falha por outro redundante previamente disponibilizado, ou seja, em standby, sem a intervenção humana ou aviso prévio.

[10] Grupo de dois ou mais servidores usados como *host* de um mesmo site. *Web farms* aumenta a capacidade de um *site* e promove disponibilidade ao agregar redundância contra falhas. *Web farms* são utilizados de forma geral para atender *sites* de alto tráfego e/ou com missões de atendimento crítico.

computadores juntos, preferencialmente de baixo custo, agindo como um só, cada um monitorando os outros e assumindo seus serviços caso algum deles venham a falhar.

2.6.3.1.3 Combinação HA & Load Balance

Como o próprio nome diz combina as características dos dois tipos de *cluster*, aumentando assim a disponibilidade e a escalabilidade de serviços e recursos. Este tipo de configuração de *cluster* é bastante utilizado em servidores *web*, *mail*, *news* ou *FTP*.

2.6.3.1.4 Processamento Distribuído ou Processamento Paralelo

Este modelo de *cluster* aumenta a disponibilidade e *performance* para as aplicações, particularmente as grandes tarefas computacionais. Uma grande tarefa computacional pode ser dividida em pequenas tarefas que são distribuídas ao redor das estações, como se fossem um supercomputador operando individualmente. Estes *clusters* são usados para computação científica ou análises financeiras, tarefas típicas para exigência de alto poder de processamento.

2.6.3.2 Razões para Utilização de *Cluster*

Clusters ou combinações de *clusters* são usados quando os conteúdos são críticos ou quando os serviços têm que estar disponíveis e/ou processados o mais rápido possível. *Internet Service Providers* (provedores de Internet) ou sites de comércio eletrônico freqüentemente requerem alta disponibilidade e balanceamento de carga de forma escalonável. *Clusters* paralelos são usados na indústria cinematográfica para renderização[11] de gráficos de altíssima qualidade e animações. Na figura abaixo, *Heart Beat* são os sinais de controle trocados entre os servidores.

[11] Processo pelo qual se podem obter imagens digitais, aplicado essencialmente em programas de modelagem e animação.

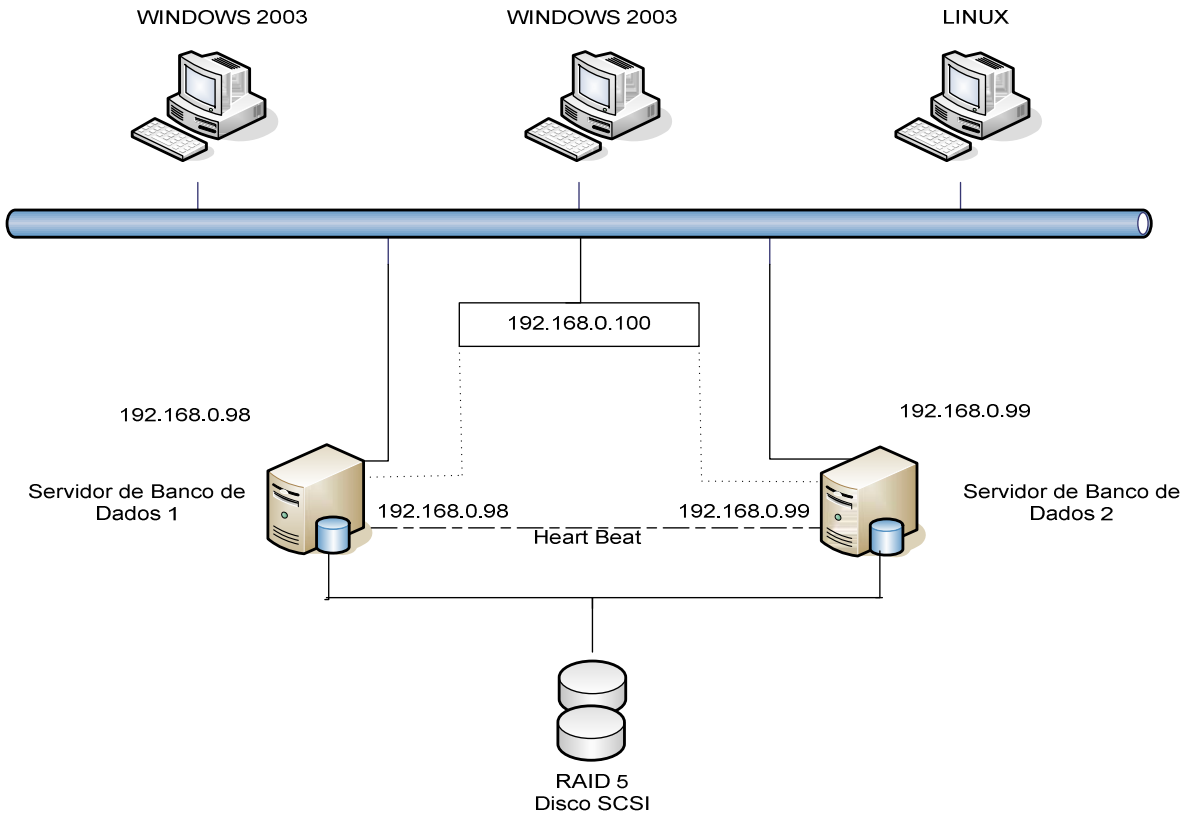


Figura 3 - *Cluster* de Alta Disponibilidade.

2.6.4 **Redundância de Roteadores**

A redundância de roteamento IP é um recurso chave na estratégia para atingir uma alta disponibilidade, uma vez que se trata de componente crítico na entrega confiável de dados, voz e vídeo de forma integrada. O objetivo da redundância de roteamento IP é proteger contra a possibilidade de falha de roteamento no *first-hop*[12] , quando o *host* de origem é incapaz de aprender dinamicamente o endereço IP de roteamento do *first-hop* alternativo.

2.6.4.1 Estabelecimento de Redundância de Roteadores

2.6.4.1.1 Proxy Address Resolution Protocol

Alguns *host* IP usam *proxy Address Resolution Protocol* (ARP) para selecionar um roteador. Quando um *host* 'A' executa o *proxy* ARP, um ARP *request* (solicitação) é enviado com o endereço IP do *host* 'B' remoto. Um roteador 'R1' na rede responde à solicitação com um ARP *reply*, contendo o endereço MAC do próprio roteador. Se este roteador 'R1' vier a falhar, o *host* 'A' continuará a enviar pacotes para o endereço MAC de 'R1'. Estes pacotes serão perdidos até que a tabela ARP de 'A' seja atualizada com a informação de um novo caminho obtido por um ARP *reque*st, cuja resposta tenha indicado o

[12] É o primeiro roteador a ser alcançado por um tráfego, no seu caminho em direção ao destino.

endereço MAC de outro roteador ‘R2’ capaz de encaminhar os pacotes no segmento de rede desejado.

2.6.4.1.2 Default Gateway

Especificar um *default gateway* em um *host* irá permitir que a ET (Estação de Trabalho) envie pacotes para outras subredes remotas através deste *default gateway*. Pode haver apenas um *default gateway* especificado em alguns sistemas operacionais, porém, em caso de falha deste *gateway*, a ET perde conexão e não consegue alcançar as subredes remotas. Apesar da infra-estrutura de rede poder rapidamente convergir e recuperar-se do erro, o *host* ‘A’ não saberá nada sobre um novo *default gateway*. Com sistemas operacionais que suportem múltiplas entradas para *default gateway*, como o Microsoft Windows, a permuta entre as entradas não é dinâmica. O sistema operacional irá enviar um *‘echo’* para cada entrada de *gateway* na ordem estabelecida, durante o *‘bootup’*. O primeiro *gateway* que responder, será usado como *default gateway*. Para usar outro *gateway* da lista, no caso de falha no roteamento, será necessário reiniciar o *host*.

2.6.4.1.3 Dynamic Routing Protocol

Alguns *host* IP executam um protocolo de roteamento dinâmico como o RIP[13] ou o OSPF[14] para descobrir rotas. Entretanto, executar um protocolo de roteamento dinâmico em todos os *host* pode não ser adequado. Isto por motivos operacionais, devido ao *overhead* de tráfego administrativo gerado por medida de segurança, ou deficiência funcional do próprio protocolo para operar adequadamente em determinadas plataformas.

2.6.4.1.4 Dynamic Host Configuration Protocol

O DHCP provê um mecanismo para passar as informações de configuração IP para *host* numa rede TCP/IP. Um *host* se conectando à rede irá requisitar a informação de configuração IP ao servidor DHCP. Esta informação de configuração tipicamente consiste de um endereço IP e de um *default gateway*.

2.6.4.2 Protocolos de Redundância Aplicados a Roteadores

2.6.4.2.1 ICMP Router Discovery Protocol (IRDP)

Alguns novos *host* IP usam IRDP (RFC 1256) para achar um novo roteador, quando o antigo se tornou inacessível. Um *host* que utiliza IRDP escuta mensagens *multicast* de *hello* do roteador configurado para uso. O *host* chaveia para um roteador alternativo quando este

[13] Routing Information Protocol – Protocolo de roteamento que utiliza o conceito de broadcast para enviar sua tabela de roteamento para todos os vizinhos.

[14] Open Shortest Path First – Protocolo de roteamento onde todos os roteadores possuem todos os links da rede registrados numa tabela de roteamento montada pelo próprio protocolo.

não mais recebe as mensagens de *hello*. IRDP transmite uma mensagem *default* de advertência entre sete e dez minutos. O tempo de vida *default* é de 30 minutos. Este *timer default* significa que o IRDP não está ajustado para detectar falhas no *first-hop*. Para configurar o protocolo IRDP, basta habilitá-lo numa interface específica e os parâmetros *default* serão aplicados.

2.6.4.2.2 Hot Standby Router Protocol (HSRP)

Uma forma de se obter próximo a 100% de disponibilidade de uma estrutura de redes é usando o HSRP, protocolo proprietário da CISCO (RFC-2281). O HSRP provê redundância para endereço IP garantindo que o tráfego do usuário seja imediatamente recuperado, de forma transparente, de uma falha no *first-hop*. Compartilhando um endereço IP e um endereço MAC, um grupo de dois ou mais roteadores pode operar como um único denominado roteador virtual. Este grupo é conhecido como grupo HSRP ou grupo *standby*. Um único roteador do grupo é escolhido para ser o responsável pelo encaminhamento dos pacotes que os *host* enviam para o roteador virtual. Para minimizar o tráfego na rede, apenas o roteador ativo e o roteador em *standby* enviam mensagens HSRP periódicas, quando estiver completo o processo de definição do papel de cada roteador. Se o roteador ativo falhar, o roteador *standby* passa a operar como o roteador ativo. Se o roteador *standby* falha ou se torna o roteador ativo, então um terceiro roteador é escolhido para se tornar o roteador *standby*. Os *host* continuam a enviar pacotes para um IP consistente e um endereço MAC virtual. A troca de papeis entre os roteadores é transparente para as ET envolvidas. Em algumas LANs podem coexistir múltiplos grupos *Hot Standby*. Cada grupo simula um roteador virtual. Roteadores individuais podem participar de vários grupos. Neste caso, o roteador mantém estados e tempos separados para cada grupo. Cada grupo *standby* possui um endereço IP e um endereço MAC virtual.

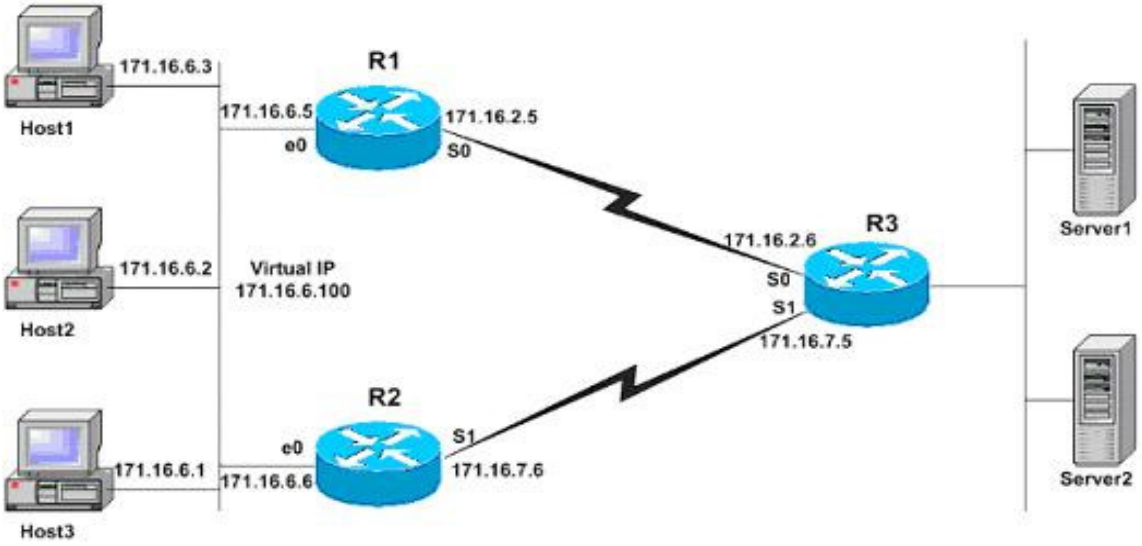


Figura 4 - Operação do HSRP

2.6.4.2.3 Virtual Router Redundancy Protocol (VRRP)

O VRRP é um protocolo proposto pelo IETF para tornar-se padrão de referência (RFC 2338) de forma similar ao protocolo HSRP. Como solução padrão introduzido em 1998, o VRRP é agora disponibilizado para prover interoperabilidade de equipamentos de fabricantes diversos.

Uma redundância de roteamento IP é designada para permitir a solução transparente contra falhas no roteador de *first-hop*. Tanto o HSRP como o VRRP habilitam dois ou mais serviços para trabalharem juntos em um grupo, compartilhando um endereço IP virtual. O endereço IP virtual é configurado em cada uma das ET como o endereço de *default gateway* e é armazenado no *cache* ARP do *host*. No grupo HSRP ou VRRP, um roteador é eleito para gerenciar todas as requisições enviadas para o endereço IP virtual. O grupo HSRP possui um roteador ativo, pelo menos um roteador em *standby* e talvez alguns outros ouvindo. O grupo VRRP possui um roteador *master* e um ou mais roteadores *backup.*

Quando um grupo é inicializado, mensagens são trocadas para eleger o roteador ativo ou *master*. Nestas mensagens são trocadas informações do tipo: identificador do grupo, prioridade, endereço IP virtual e o intervalo do aviso de *hello*. Os roteadores de um grupo permanecem trocando estas mensagens num intervalo pré-configurado. No HSRP ambos os roteadores, tanto o ativo quanto o em *standby*, enviam mensagens de *hello* periódicas. No VRRP apenas o roteador *master* envia mensagens periódicas, conhecidas como ‘aviso’. Usando a informação contida nestas mensagens o roteador *standby* ou *backup* pode determinar quando ele deve assumir como roteador ativo ou *master* de um determinado

grupo. Se uma mensagem de *hello* do roteador ativo ou *master* não for recebida no intervalo definido, o roteador *standby* ou *backup* automaticamente assumirá toda a tarefa do roteador ativo ou *master*. Quando estes se tornarem disponíveis outra vez enviarão uma mensagem de *hello* e recuperarão do papel de roteador ativo ou *master*. Tudo isto é transparente para o usuário final. A conectividade é mantida com mínima ou nenhuma perda de tráfego e funcionalidade.

A CISCO recomenda usar o HSRP porque provê uma tecnologia com características superiores de convergência. O VRRP é recomendado apenas para os casos em que a interoperabilidade entre subredes com equipamentos de fabricantes diferentes é exigida. A customização do comportamento do VRRP é opcional. Assim que um grupo é habilitado, este grupo se torna operacional. O VRRP deve ser customizado sempre antes de ser habilitado. Caso contrário um roteador pode se tornar *master* virtual antes que a customização se complete.

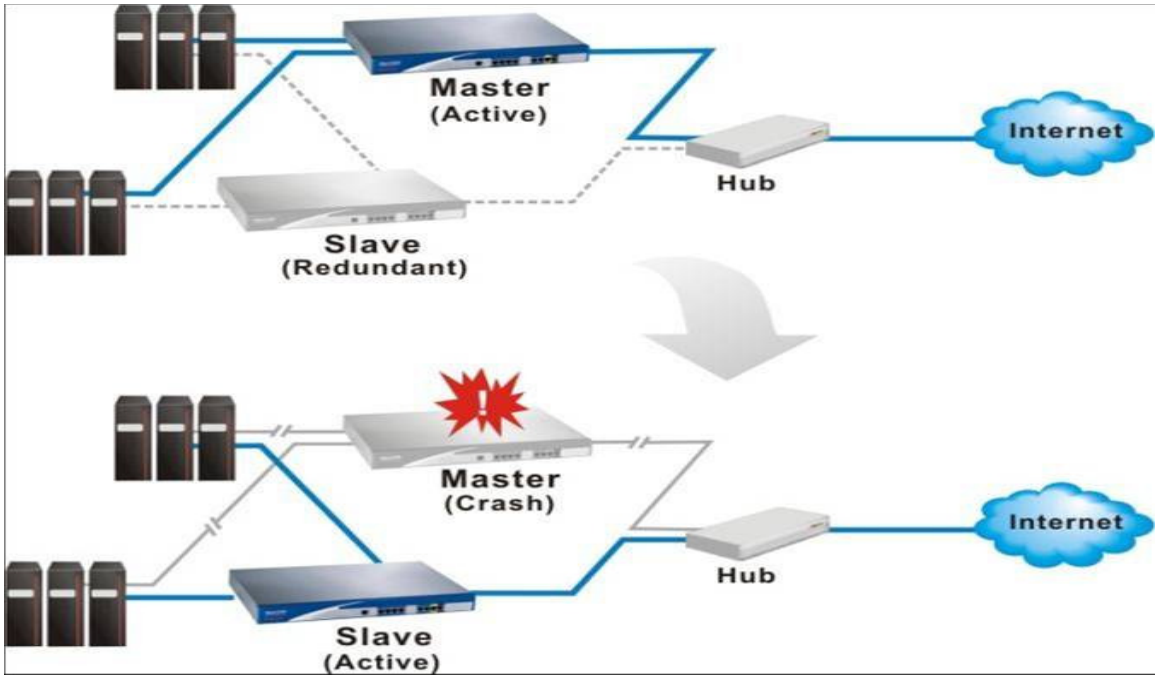


Figura 5 - Operação do VRRP.

2.6.4.2.4 Gateway Load Balancing Protocol (GLBP)

Assim como o HSRP e VRRP, o GLBP também oferece um método para prover um caminho ininterrupto redundante para tráfego IP, compartilhando protocolo e endereço MAC entre *gateway* redundantes. O GLBP também permite que um grupo de roteadores

compartilhe a carga do *default gateway* de uma LAN. Este processo agrega *performance* possibilitando um melhor uso dos recursos da rede, disponibilizando múltiplas alternativas de caminhos, além de acrescentar confiabilidade e disponibilidade ao eliminar o roteador *first-hop* como SPOF. O GLBP habilita um roteador para automaticamente assumir a função de qualquer outro roteador *gateway*.

O GLBP permite que o tráfego de uma subrede comum seja encaminhado por *gateway* múltiplo redundante, enquanto usa um simples endereço virtual IP. Ele provê o mesmo nível de capacidade de recuperação de falha de *first-hop* oferecido pelos protocolos HSRP e VRRP.

2.6.4.2.5 Single Router Mode (SRM) Redundancy

Usando a redundância SRM, apenas o roteador designado como ativo é visível para a rede em qualquer momento. O roteador não designado é inicializado e participa da configuração da sincronização, que é habilitada quando da entrada em operação do SRM. A configuração do roteador não designado é exatamente a mesma do roteador designado, porém as interfaces do primeiro são mantidas em estado de *line-down* e não são visíveis para a rede. Processos como protocolos de roteamento são criados no roteador não designado e no designado. Todas as interfaces dos roteadores não designados ficam no estado *line-down* e não trocam atualizações com a rede. Quando o roteador designado falha, o roteador não designado altera seu estado para roteador designado, o estado da interface muda para *link up* e o roteador monta sua tabela de roteamento de forma a cumprir seu novo papel.

2.6.4.2.6 Common Address Redundancy Protocol (CARP)

CARP é o Protocolo de Redundância de Endereço Comum (Common Address Redundancy Protocol). Seu objetivo principal é permitir que múltiplos *hosts* no mesmo segmento de rede compartilhem um endereço IP. O CARP é uma alternativa livre e segura ao *Virtual Router Redundancy Protocol* (VRRP) e ao *Hot Standby Router Protocol* (HSRP), funciona permitindo que um grupo de *hosts* no mesmo segmento de rede compartilhe um endereço IP. Este grupo de *hosts* é referenciado como um *grupo de redundância*. Ao *grupo de redundância* é atribuído um endereço IP que é compartilhado entre os membros do grupo. Dentro do grupo, um host é designado como *master* e o resto como *backup*. O *host master* é o que atualmente "segura" o IP compartilhado; ele responde a qualquer tráfego ou requisições ARP direcionadas para ele. Cada *host* pode pertencer a mais que um *grupo de redundância* por vez.

O *host master* no grupo envia regularmente anúncios à rede local, assim os *hosts backup* sabem que ele ainda está ativo. Se os *hosts backup* não ouvirem um anúncio do *master* por um determinado período de tempo, um deles tomará conta dos deveres do *master*.

2.6.4.2.7 Redundância de Firewall Utilizando CARP

Um uso comum para o CARP é criar um grupo de *firewall* redundantes. O IP virtual, que é atribuído ao *grupo de redundância*, é configurado nas máquinas clientes como o gateway padrão. Caso o *firewall* sofra uma falha ou seja desligado o IP se moverá para um dos *firewall backup* e o serviço vai continuar sem ser afetado. Combinando as características do CARP com as de um programa chamado PFSYNC[15], pode-se criar um *cluster* de *firewall* completamente redundante e com alta disponibilidade. Enquanto o CARP trata o *failover* automático de um *firewall* para outro, o PFSYNC sincroniza a tabela de estados entre todos os *firewalls*. Caso aconteça um *failover* o tráfego pode fluir de forma ininterrupta através do novo *firewall master.*

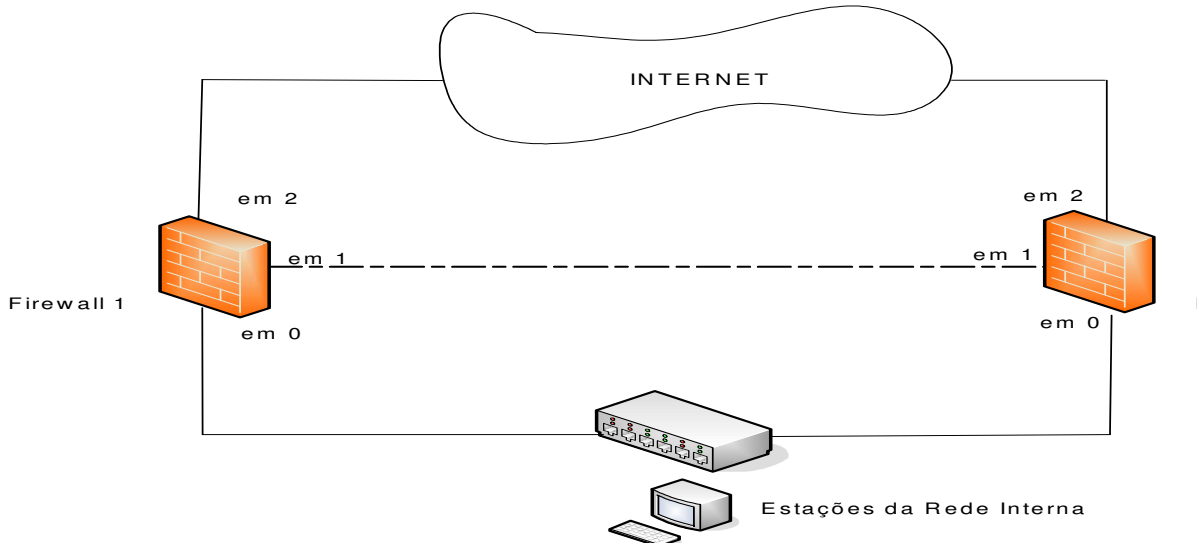


Figura 6: Exemplo de dois *firewall*, fw1 e fw2.

Os *firewall* estão conectados diretamente usando um cabo *crossover* em "*em1*". Ambos estão conectados à LAN em "*em0*" e a uma conexão WAN/Internet em "*em2*".

---

[15] Programa de computador usado para sincronizar estados do *firewall* entre as máquinas em que funciona o filtro de pacotes para a disponibilidade elevada. Usando-se junto com o CARP, quando a máquina principal no conjunto do *firewall* falha, a máquina *backup* pode aceitar conexões atuais sem perda.

2.6.5 **Redundância de Servidores**

Considerados os equipamentos de maior importância de uma estrutura de rede, os servidores devem receber atenção especial nos quesitos disponibilidade e confiabilidade. Desta forma eles são freqüentemente equipados com dispositivos redundantes, possibilitando acesso ininterrupto. Recomenda-se o estabelecimento de prioridades dentre os servidores presentes na rede, de forma a alinhar os investimentos necessários.

Quadro 2 – Servidores passíveis de receberem redundância.

DHCP	E-MAIL	ANTISPAM
DNS	PROXY	ANTIVÍRUS
VPN	DOMÍNIO	ACESSO REMOTO
FIREWALL	ARQUIVOS	BACKUP
WEB	BANCO DE DADOS	REPLICAÇÃO DE DADOS
IMPRESSÃO	AUTENTICAÇÃO DE ACESSO	FTP

2.6.5.1 Server Load Balancing (SLB)

SLB é uma solução baseada no IOS que define um servidor virtual como representante de um grupo de servidores reais em uma fazenda. Este ambiente permite conectar clientes a um servidor virtual. O endereço IP do servidor virtual é configurado como endereço de *loopback* ou endereço IP secundário em cada um dos servidores reais. Quando um cliente inicia uma conexão com o servidor virtual, a função SLB escolhe um servidor real para que forneça a conexão, baseado num algoritmo de balanceamento de carga. A rede adquire escalabilidade e disponibilidade quando servidores virtuais representam fazendas de servidores. O acréscimo de novos servidores e a remoção de servidores por falhas podem ocorrer a qualquer momento, sem afetar a disponibilidade do servidor virtual.

2.6.6 **Redundância no Suprimento de Força**

Por ter que operar de maneira ininterrupta, alguns servidores são ligados a geradores elétricos. Outros utilizam sistemas de alimentação que continuam a alimentar o servidor caso haja alguma queda de tensão. Uma fonte de alimentação ininterrupta, também conhecida pelo acrônimo UPS, *Uninterruptible Power Supply,* é um sistema de alimentação elétrica que entra em ação alimentando os dispositivos a ele conectados caso haja interrupção no fornecimento de energia.

Redundância de suprimento de força de alimentação elétrica é um fator a ser apreciado em situações que envolvem missão crítica de tráfego. Em sistemas com suprimento de força

redundante, as fontes devem ser da mesma potência. Alguns roteadores permitem combinar alimentação elétrica AC e DC num mesmo chassi. Um exemplo deste tipo de equipamento é o roteador CISCO 3725 que oferece a possibilidade de ser instalado o módulo CISCO 3725 *Redundant Power Supply (RPS) Interface Module*. Este módulo substitui a fonte de alimentação AC ou a fonte DC – 48 VDC instaladas no roteador. A interface conecta o aparelho ao módulo CISCO 600W *Redundant Power System* através de um cabo específico e é usada para converter e distribuir a alimentação DC fornecida por este módulo, para a voltagem DC usada pelo roteador [11].

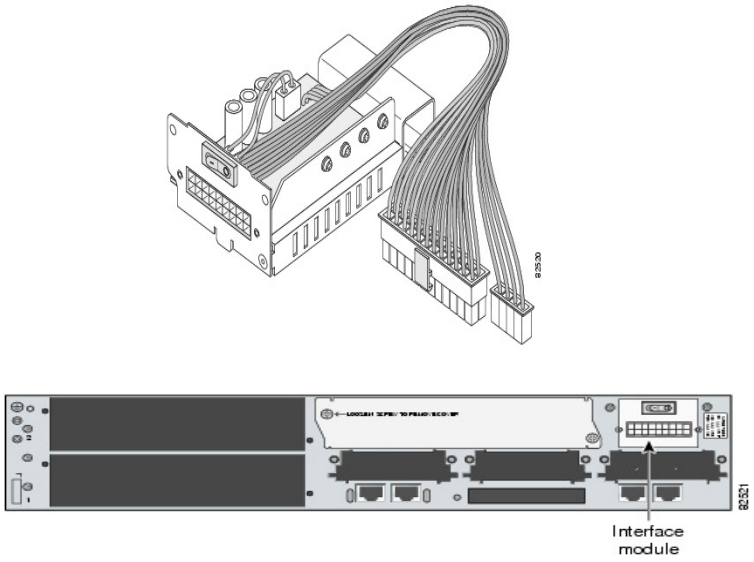


Figura 7: Modulo de Interface da fonte redundante do CISCO 3725 e sua posição no chassi

Uma vez habilitada a redundância e duas fontes de mesma potência instalada, em nenhum momento o fornecimento de energia será maior do que a capacidade de fornecimento feito por apenas uma das fontes. Se uma das fontes apresentar falha, a outra poderá assumir o fornecimento de força de todo o sistema individualmente sem problemas. Quando duas fontes de capacidades iguais são usadas, cada uma provê aproximadamente a metade da força requerida para a operação do sistema. A carga é dividida e a redundância é habilitada automaticamente. Não há necessidade de configuração de *software*.

Com a redundância habilitada e duas fontes de potências diferentes instaladas, ambas as fontes entram em operação, porém uma mensagem de *syslog* indica que a fonte de menor potência será desabilitada. Se a fonte ativa apresentar falha, a fonte de menor potência entra em operação e alguns módulos podem ser desativados, se necessário, para acomodar o menor fornecimento de energia.

Em uma configuração sem redundância, a força disponível para o sistema é uma combinação da capacidade de ambas as fontes. O sistema coloca em operação o que for possível, dentro da capacidade disponível. Entretanto, se uma fonte falhar e não houver potência suficiente para manter os módulos operantes, o sistema desliga alguns módulos. A configuração das fontes pode ser alterada para redundante ou não redundante a qualquer tempo.

2.6.7 **Protocolo IEEE 802.1D - Spanning Tree**

O *Spanning Tree* é um protocolo para sistemas baseados em *bridges/switches*, que permite a implementação de caminhos paralelos para o tráfego de rede. Utiliza um processo de detecção de *"loops"* para encontrar e desabilitar os caminhos menos eficientes (com menor largura de banda) e para habilitar o caminho redundante, menos eficiente, se o mais eficiente falhar.

O algoritmo de *Spanning Tree* determina qual é o caminho mais eficiente entre cada segmento separado por *bridges* ou *switches*. Caso ocorra um problema nesse caminho, o algoritmo irá recalcular o novo caminho mais eficiente, habilitando-o automaticamente.

O protocolo S*panning Tree* possibilita que os equipamentos sejam configurados em uma topologia em árvore (sem *loop*), permitindo que o administrador da rede possa "forçar" que um determinado equipamento seja escolhido como a raiz da árvore.

As especificações do protocolo *Spanning Tree* são padronizadas pelo IEEE, dentro do conjunto das normas IEEE 802.1D.

3 METODOLOGIA DE PESQUISA

Neste estudo é adotado o método qualitativo. Serão consideradas as informações significativas obtidas através do levantamento técnico do material bibliográfico físico e eletrônico obtido.

O juízo de valor e a conclusão serão formados a partir dos quesitos especificados nos tópicos seguintes.

3.1 TIPO DE PESQUISA

Quanto ao objetivo, esta é uma pesquisa parcialmente exploratória por tratar o recurso da redundância como o tema central de forma pouco explorada na literatura técnica, ao mesmo tempo em que se torna descritiva por pretender oferecer contornos descritivos das principais características dos fatores que levam ao uso da redundância numa LAN, em busca da total disponibilidade e confiabilidade .

Quanto aos meios utilizados, conforme acima exposto, foram realizadas pesquisas bibliográficas documentais, com levantamento e seleção de material técnico apropriado.

3.2 PROPOSTA DE LEVANTAMENTO TÉCNICO

Será aqui exposta a sugestão de elaboração da Planilha de Prioridades de SPOF (PPS)**,** como forma de otimizar a aplicação dos recursos redundantes na eliminação de SPOF. A elaboração da planilha respeitará as seguintes fases: Avaliação da Instalação; Identificação de *Single Point of Failure*; Estabelecimento de Riscos e Prioridades; Estabelecimento de Linhas de Ação; Execução/Testes; Análise e Conclusão. Estas fases serão detalhadas a seguir.

3.2.1 **Avaliação da Instalação**

Após a definição da instalação a ser apreciada, esta será tema de avaliação prévia quanto ao seu porte, a sua estruturação, modo de operação e quanto aos componentes presentes. Posteriormente é iniciada a fase de Identificação de SPOF. Por exemplo, a Figura 8 ilustra a configuração básica e típica de um sistema de comunicações de dados simples, onde um servidor qualquer atende a três estações através de um equipamento de conectividade. Neste caso tanto o servidor quanto o referido equipamento de conectividade são considerados SPOF.

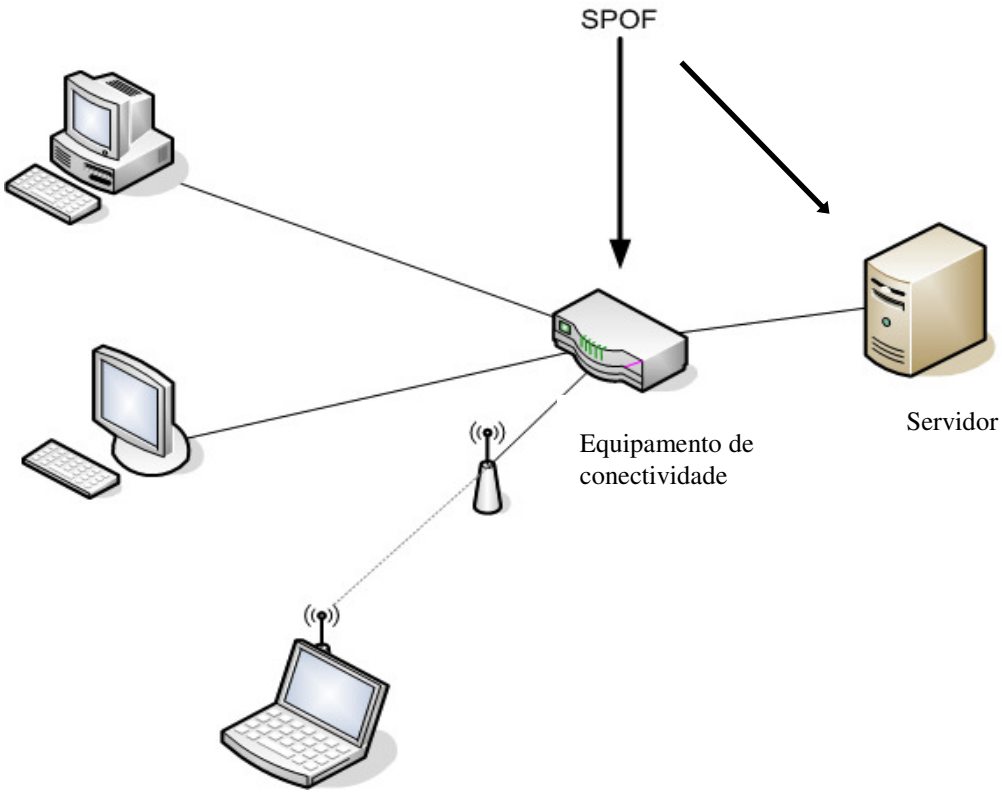


Figura 8 – Esquema básico de uma rede com roteador e servidor como SPOF.

3.2.2 **Identificação de Single Point of Failure (SPOF)**

Um SPOF é um ponto único de falha ou ponto crítico de falha. Trata-se de uma tradução vinda da língua inglesa da expressão *Single Point of Failure* (*SPOF*) para designar um local num sistema informático que, caso falhe, provoca a falha de todo o sistema. Assim, serão identificados os componentes que, em caso de falhas, comprometerão o funcionamento de toda a rede. Nestes pontos, eventualmente, cabe a utilização dos recursos de **redundância,** de forma a oferecer maior disponibilidade e confiabilidade à instalação. No caso da Figura 8, poderia se considerar que o equipamento central da estrela, seja ele um roteador, *switch* ou *hub,* deveria receber uma instalação redundante de forma que, em caso de falha, a rede não seja desabilitada por completo. Da mesma forma, havendo um servidor entre os nós, este também seria um SPOF identificado como merecedor de aplicação de redundância**,** em algum nível a ser determinado.

3.2.3 **Estabelecimento de Disponibilidades e Riscos**

A partir da identificação dos pontos de falha na etapa anterior, deve-se definir a Disponibilidade de cada componente, conforme as instruções do item 2.2 e os Riscos aos quais a instalação estará exposta no caso de inoperância dos SPOF identificados.

3.2.4 **Estabelecimento de Linhas de Ação**

Dentro das prioridades estabelecidas, são traçadas as estratégias para reduzir os riscos de falhas dos referidos SPOF. Ou seja, são definidos métodos para atacar os problemas de fragilidade da rede para que, dentro das disponibilidades técnicas e de recursos do administrador, seja agregada robustez. Cada estratégia escolhida passa a ser uma Linha de Ação e recebe um número identificador, da mais adequada[16] que será a de número 1, para a menos adequada, a de número "n". Assim, cada SPOF terá de uma a "n" Linhas de Ação, acompanhadas de orçamento, passíveis de eliminar a possibilidade de falha naquele ponto.

3.2.5 **Execução, Testes, Custos e Prioridades**

Definidas as Linhas de Ação para cada SPOF na fase anterior, estas serão implementadas ou simuladas nesta fase de execução e testadas dentro das possibilidades do ambiente. Como resultado poderá ser definido quais Linhas de Ação são exequíveis e aceitáveis. Ao final desta etapa o administrador terá as informações necessárias para o levantamento dos Custos e das Prioridades da execução de cada Linha de Ação. O estabelecimento de Prioridades pode variar com os critérios de cada empresa. São considerados fatores relevantes: a gravidade dos riscos, a disponibilidade medida de cada componente dentro da atividade fim da empresa, os resultados dos testes de simulação e os custos de implementação das Linhas de Ação. Há possibilidade de assumir a mesma prioridade para Linhas de Ação diferentes, isto para os casos de serviços que devam ser realizados paralelamente. Linhas de Ação diferentes para eliminar um mesmo SPOF podem ter prioridades diferentes, se tiverem diferentes custos. È importante ressaltar que seja qual for o critério de estabelecimento da prioridade esta deve variar da maior, com valor igual a 1, até a menor que deverá ter qualquer valor superior a 1, ou seja, quanto maior a prioridade, menor o seu valor. Pode haver o estabelecimento de uma mesma prioridade para diferentes SPOF.

3.2.6 **Análise e Conclusão**

Após o registro dos resultados dos testes na fase anterior, estes são analisados na fase de Análise e Conclusão. No final desta fase, deverá ser emitido um parecer técnico

---

[16] Características desejáveis de uma solução: adequada – quando através desta solução é possível alcançar o resultado desejado; exequível – quando uma solução adequada é possível de ser executada diante dos recursos disponíveis; e aceitável – quando o resultado a ser obtido por uma solução adequada e exequível é compensadora no quesito custo x benefício, resolvendo o problema.

conclusivo com a análise feita sobre cada Linha de Ação de cada SPOF identificado nas fases anteriores. O parecer obtido deverá constar no campo *Execução/Testes* da PPS ou em Relatório Complementar (este Relatório não receberá apreciação detalhada nesta monografia, ficando a critério do administrador sua confecção ou não e a sua forma). Assim, pode-se chegar a uma conclusão prática de como devem ser aplicados os recursos no sentido de garantir confiabilidade e disponibilidade à estrutura de serviço da rede. Como exemplo de objetivo a ser alcançado, é ilustrado na Figura 9 a configuração de um sistema de alta disponibilidade. Como se pode observar, não existe um único ponto nesta arquitetura que, ao falhar, implique na indisponibilidade de algum outro ponto da estrutura.

O fato de ambos servidores se encontrarem em funcionamento e ligados à rede não significa que se encontrem a desempenhar as mesmas tarefas, pois pode ser realizado um *balanceamento de carga*.

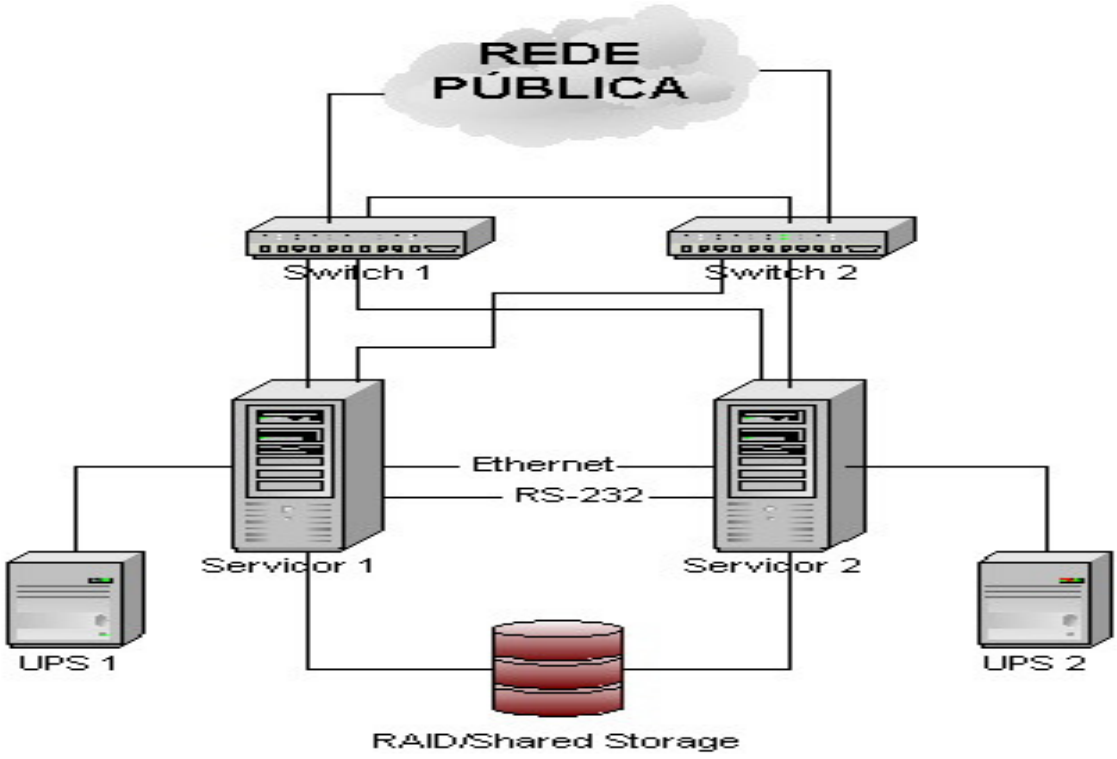


Figura 9 - Arquitetura clássica de um sistema *dual-node* de alta disponibilidade

3.2.7 **Elaboração da Planilha de Prioridades de SPOF (PPS)**

Como resultado das fases anteriores, foram reunidas as informações necessárias para a elaboração da PPS. São elas: a *Identificação* do SPOF; o *Componente* envolvido; a *Localização;* a *Disponibilidade* histórica de acordo com o MTBF e o MTTR; os *Riscos;* a

Prioridade de eliminação de cada SPOF em relação aos demais, diante da gravidade dos *Riscos* que representa; as respectivas *Linhas de Ação* previstas; os resultados dos testes de *Execução* de cada Linha de Ação; e os *Custos* estimados para implementar cada uma. Os custos podem ser alinhados conforme necessidade do usuário, podendo ser incluído o gasto com Homem/Hora.

A PPS deve funcionar como uma ferramenta de apoio à decisão de **onde, quando e como** aplicar de forma otimizada o recurso da redundância. Para isto ela deve possuir as informações necessárias sobre cada SPOF. O apoio da Planilha também ocorre no momento em que os SPOF estão registrados e identificados, assim, em caso de interrupção do serviço, a PPS indica **onde** estão os pontos a serem checados e suas características. **Quando** houver possibilidade, o campo *Prioridade* indica a ordem de eliminação do SPOF. As Linhas de Ação e os resultados dos respectivos testes de *Execução* realizados caracterizam **como** os referidos pontos devem ser atacados e quais são os *Custos* envolvidos. A partir do momento em que um SPOF é eliminado, este deve ser retirado da PPS e a coluna Prioridade deverá ser atualizada. A PPS deve possuir um perfil dinâmico e não estático, permitindo assim constantes reavaliações sobre a consistência de seu conteúdo. A coluna *Custos* poderá ser representada por qualquer moeda e/ou indexada com cotações monetárias internacionais.

Quadro 3 : Exemplo de PPS

ID	Componente	Disponibilidade	Riscos	L.Ação	Execução/Testes	Custos	Prioridade
				1-			
				2-			
				3-			
				1-			
				2-			

4 DESCRIÇÃO DE CASO

De forma a ilustrar a metodologia descrita no capítulo anterior, é exposto aqui um pequeno exemplo da elaboração e da aplicabilidade da planilha PPS.

Considera-se a figura abaixo como uma seção de rede a ser avaliada quanto à disponibilidade e confiabilidade do serviço:

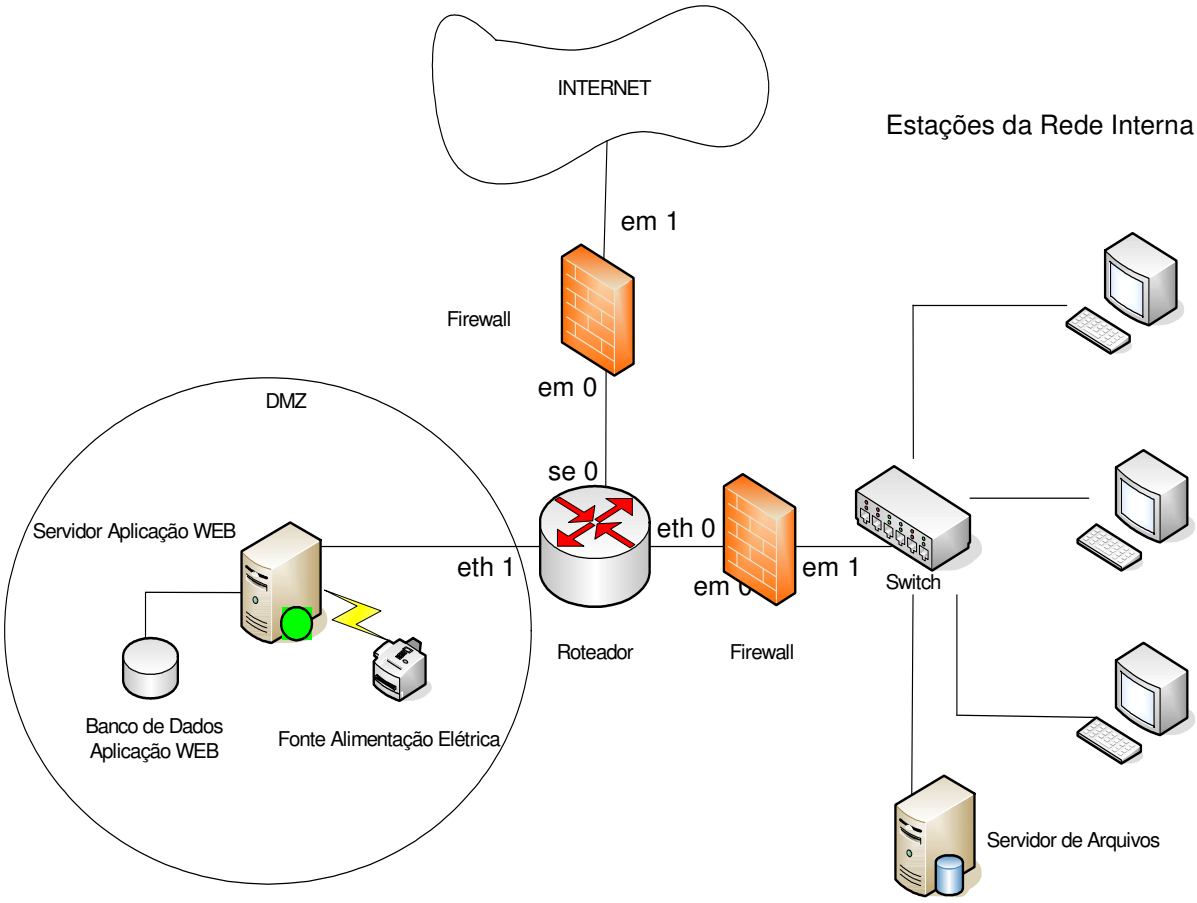


Figura 10 : Exemplo de Seção de Rede para avaliação

Como pode ser observado na Figura 10, fica exposto para ser analisado no próximo capítulo um ambiente primário composto de um roteador de borda que viabiliza a conexão, via internet, para um servidor de aplicação *web*, localizado em zona desmilitarizada. O mesmo roteador conecta a rede interna corporativa ao servidor *web* e à internet.

5 ANÁLISE DE CASO

Aplicando a metodologia descriminada no capítulo 3 e os conhecimentos teóricos constantes no capítulo 2, segue-se a avaliação da estrutura da seção de rede da Figura 9.

5.1 AVALIAÇÃO DA INSTALAÇÃO

Trata-se de uma seção estruturada de LAN composta principalmente por: um Roteador estabelecendo o backbone que conecta a rede corporativa à internet através de conexão banda larga de 4 MBs; um Servidor *WEB* com Banco de Dados em DMZ[17], alimentado por uma única Fonte de 120V/1KVA; dois *Firewall;* um *Switch* conectando dezoito Estações de Trabalho e um Servidor de Arquivos com dados de gestão e conduta administrativa da empresa; todos os *links* cabeados com UTP CAT 5 trafegando dados gerenciais e voz a 100 MBs; não há qualquer redundância aplicada nestes pontos.

5.2 IDENTIFICAÇÃO DE SPOF

Sem maiores detalhamentos, são observados os seguintes pontos sujeitos a falhas: o Roteador; o *Switch;* os dois *Firewall;* o Servidor *WEB*; o Banco de Dados; os *Links* Roteador-Internet, Roteador-Servidor *WEB*, Roteador-Switch e Switch-Servidor de Arquivos; a Fonte de Alimentação do Servidor *WEB* e o Servidor de Arquivos, todos com potencial para causar prejuízos operacionais e interrupções de serviço em caso de inoperância. A identificação do ponto pode sugerir a sua localização, assim, considerando que o *switch* é localizado no Departamento de Recursos Humanos do terceiro andar e o CPD fica no primeiro andar, a identificação de cada ponto será a seguinte: três algarismos para o andar, três letras para a identificação do setor e três algarismos para o número do ponto.

Quadro 4: Montagem PPS – Colunas Identificação e Componente.

ID	Componente
001CPD-001	Roteador CISCO 2500
003RHU-001	*Switch* D-link
001CPD-002	*Firewall* porta Roteador eth0 *stateful*[18]
001CPD-003	*Firewall* porta Roteador se0 *stateful*
001CPD-004	Servidor *WEB*
001CPD-005	Banco de Dados aplicação *WEB*
001CPD-006	*Link* Roteador-Internet
001CPD-007	*Link* Roteador-Servidor *WEB*

[17] Área de rede que permanece entre a rede interna de uma organização e uma rede externa, em geral a internet. Geralmente a DMZ contém equipamentos apropriados para o acesso à internet, como servidores WEB, FTP, SMTP e DNS.

[18] *Firewall stateful* tem a capacidade de identificar o protocolo dos pacotes transitados e "prever" as respostas legítimas. Na verdade, o *firewall* guarda o estado de todas as últimas transações efetuadas e inspecionava o tráfego para evitar pacotes ilegítimos.

ID	Componente
001CPD-008	*Link* Roteador-*Switch*
001CPD-009	*Link Switch* –Servidor Arquivos
001CPD-010	Fonte Alimentação Servidor *WEB*
001CPD-011	Servidor Arquivos

5.3 ESTABELECIMENTO DE DISPONIBILIDADES E RISCOS

A título de exemplo foi considerada a disponibilidade anual, calculada conforme o item 2.2, diante do histórico de avarias de cada ponto. Nesta simulação são relatados os Riscos básicos. Em casos reais é desejável um maior nível de detalhamento.

Quadro 5: Montagem PPS – Colunas: Identificação, Disponibilidade e Riscos.

ID	Disponibilidade	Riscos
001CPD-001	**A-** 99,17 %	**B-** Perda disponibilidade conexão Internet e Serv. *WEB*
003RHU-001	**A-** 95,36 %	Perda de conexão das ET a todos os serviços de rede
001CPD-002	96,98 %	Perda de filtro de entrada/saída de pacotes de Internet
001CPD-003	96,03 %	Perda de filtro de entrada/saída de pacotes rede interna
001CPD-004	**A-** 95,04 %	**C-** Perda de disponibilidade de sistemas WEB
001CPD-005	96,76 %	**C-** Perda de disponibilidade de sistemas WEB
001CPD-006	97,54 %	Perda de disponibilidade de conexão Internet
001CPD-007	98,05 %	**C-** Perda de disponibilidade de sistemas WEB
001CPD-008	97,99 %	**B-** Perda disponibilidade conexão Internet e Serv. *WEB*
001CPD-009	97,00 %	**D-** Perda de disponibilidade dos Sistemas Corporativos
001CPD-010	98,23 %	**C-** Perda de disponibilidade do serviço *WEB*
001CPD-011	98,43 %	**D-** Perda de disponibilidade dos Sistemas Corporativos

Pode-se observar no quadro 5 que algumas linhas da coluna “Disponibilidade” são precedidas da letra “A” e algumas linhas da coluna “Riscos” são precedidas das letras “B”, “C” e “D”. Estas letras são utilizadas para identificação das respectivas linhas na explicação a seguir. As letras “B”, “C” e “D” da coluna Riscos, por exemplo, indicam que alguns riscos podem ter a mesma descrição, isto porque a falha de SPOF diferentes podem ocasionar exatamente o mesmo efeito nocivo à instalação.

Para se obter a Disponibilidade, aplica-se a fórmula demonstrada no item 2.2:

$$((MTBF) / (MTBF + MTTR)) . 100\% ;$$

As linhas com a letra “A” da coluna “Disponibilidade” foram preenchidas baseadas nas seguintes informações:

- O roteador CISCO (ID = 001CPD-001) tem sua operação interrompida de 10 em 10 dias, em média, por problemas diversos e a cada parada são exigidas 2 horas para o retorno à atividade normal. Assim, o MTBF do equipamento é de 10 x 24 horas, que equivale a 240 horas de operação entre cada falha. O MTTR do mesmo é de 2 horas,

ou seja, para cada falha são consumidas, em média, 2 horas para reparo e retorno à operação. Então:

((240) / (240 + 2)) .100% = 99,17%.

- O Switch D-Link (ID = 003RHU-001) por ser mais antigo e de qualidade inferior, possui um índice de avarias maior. Seu MTBF é de 72 horas e seu MTTR é de 3 horas e 30 minutos, assim o seu índice de disponibilidade é de:

((72) / (72+ 3,5)) . 100% = 95,36%.

- O Servidor WEB (ID = 001CPD-004), o mais instável da PPS, tem sua operação interrompida, por problemas de *hardware*, de dois em dois dias e para recolocá-lo em operação são perdidas, em média, 2 horas e 30 minutos. Sua disponibilidade é de:

((48) / (48 + 2,5)) .100% = 95,04%.

5.4 ESTABELECIMENTO DE LINHAS DE AÇÃO (LA)

Trata-se da parte mais sensível, onde são realizados levantamentos de alternativas para eliminação dos SPOF.

Quadro 6: Montagem PPS – Colunas: Identificação e Linhas de Ação.

ID	Linhas de Ação
001CPD-001	1- Aquisição novo roteador CISCO e implementação do HSRP
	2- Aquisição novo roteador e implementação do VRRP
	3- Implementação de roteamento alternativo por PC
003RHU-001	1-Aquisição de novo *switch* e implementação de spanning tree
001CPD-002	1- Criação de *cluster de firewall* utilizando CARP e PFSYNC
001CPD-003	
001CPD-004	1- Duplicação de Serv. *WEB* com endereço IP comum e SLB
	2- Duplicação de Serv. *WEB CLUSTER e LOAD BALANCE*
001CPD-005	1- Implementação de RAID 5 ou 1 com discos SCSI
001CPD-006	1-Implementação de *links* paralelos com *Spanning Tree*
001CPD-007	
001CPD-008	2-Implementação de *Links Resilientes*
001CPD-009	
001CPD-0010	1- Aquisição de No Break e fontes redundantes UPS
	2- Implementação de fontes redundantes UPS
001CPD-0011	1- Duplicação de Serv e configuração com CLUSTER HA

5.5 EXECUÇÃO, TESTES, CUSTOS E PRIORIDADES

Após a definição das Linhas de Ação entramos na fase de Execução e Testes. Respeitando as restrições impostas para cada caso, as Linhas de Ação devem ser executadas e testadas, tendo os resultados registrados na PPS. Para constar na PPS a Linha de Ação já deverá ser considerada adequada, ou seja, capaz de resolver o problema, assim nesta fase a

Linha de Ação é testada no sentido da sua exeqüibilidade e aceitabilidade. A etapa de Execução e Testes fornece o respaldo necessário para que se possa estimar os Custos de implementação e as Prioridades de implantação. É de grande importância que o resultado dos testes sejam explícitos na PPS de forma sintética e, se necessário, detalhado em Relatório Complementar, de formato e conteúdo definidos pelo administrador. No quadro 7, as conclusões mais extensas contidas na coluna "Execução/Testes" podem compor o Relatório Complementar, à critério do administrador, permanecendo na PPS apenas as declarações resumidas, conforme pode ser constatado mais adiante no quadro 8. O conjunto de informações servirão como referência técnica de apoio e orientação à decisões futuras. Na PPS, a abreviatura EA significa exequível e aceitável, ou seja, é possível executar a Linha de Ação e uma vez executada, esta será aceita como solução, diante das circunstâncias observadas na fase de Execução/Testes. Uma Linha de Ação pode ser perfeitamente exequível , porém não aceita por demandar, por exemplo, grande volume de recursos financeiros e/ou disponibilidade de tempo além das possibilidades.

Quadro 7: Montagem PPS – Colunas: Identificação, Execução/Testes, Custos e Prioridade.

ID	Execução/Testes	Custos	Prio
001CPD-001	EA; Obtido por empréstimo, o roteador utilizado atendeu às expectativas, operou com HSRP como ativo e *standby.* Eliminou falhas *first-hop*	R$8.500,00	04
	Não aceitável, gera inoperância	XXX	
	Não exeqüível, problemas de configuração do *firewall*	XXX	
003RHU-001	EA; Adaptado switch 3COM 3CBLSG24 gerenciável, configurado *spanning tree* e simulado necessidade caminhos alternativos.	R$2.600,00	02
001CPD-002	EA; Pequeno conflito de IP inicial que uma vez resolvido permitiu operação perfeita do CARP com PFSYNC, sem perda de conexões.	R$100,00	11
001CPD-003	EA; Executado o mesmo teste bem sucedido do 001CPD-002.	R$100,00	11
001CPD-004	EA; aprovado o servidor criado com SLB	R$12.000,00	07
	Exeqüível e NÃO Aceitável; alto custo	R$16.000,00	12
001CPD-005	EA; não há outra alternativa até então	R$6.000,00	10
001CPD-006	EA; links estabelecidos com consistência	R$250,00	06
001CPD-007		R$250,00	08
001CPD-008		R$250,00	05
001CPD-009		R$250,00	03
001CPD-010	EA; apesar do custo deve ser aplicada	R$ 2.500,00	09
	EA; inseguro na falta de energia elétrica	R$ 950,00	13
001CPD-011	EA; implementada satisfatoriamente	R$ 15.000,00	01

5.6 ANÁLISE E CONCLUSÃO

Neste ponto a PPS começa a assumir seu perfil definitivo. No caso de confecção de Relatório Complementar, sugere-se que neste sejam expostas as definições e decisões tomadas durante a fase de Execução/Testes ou quaisquer outros comentários pertinentes, como por exemplo as causas que levam um equipamento a estar mais ou menos disponível. O Relatório pode agregar valor discursivo e detalhamento técnico à PPS, também auxiliando na tomada de decisões.

Quanto à aplicabilidade da PPS, a mais evidente é relativa à disponibilização de importantes informações de auxílio à decisão para aplicação de recursos ou para a solicitação dos mesmos. Outra aplicação importante é quanto à possibilidade de efetuar observações quanto aos riscos aos quais a rede está exposta e quanto à disponibilidade dos serviços oferecidos pela mesma. A PPS foi idealizada para ser uma ferramenta de consulta rápida e dinâmica, um guia de referência de pontos críticos que devem receber supervisão e controle especial.

Com alguns detalhes omitidos, a figura 11 representa o caso analisado em configuração de alta disponibilidade, considerando ainda os *links* redundantes e os de controle, não representados. Ressalta-se que esta configuração exige investimentos que devem ser otimizados e priorizados com o auxílio da PPS.

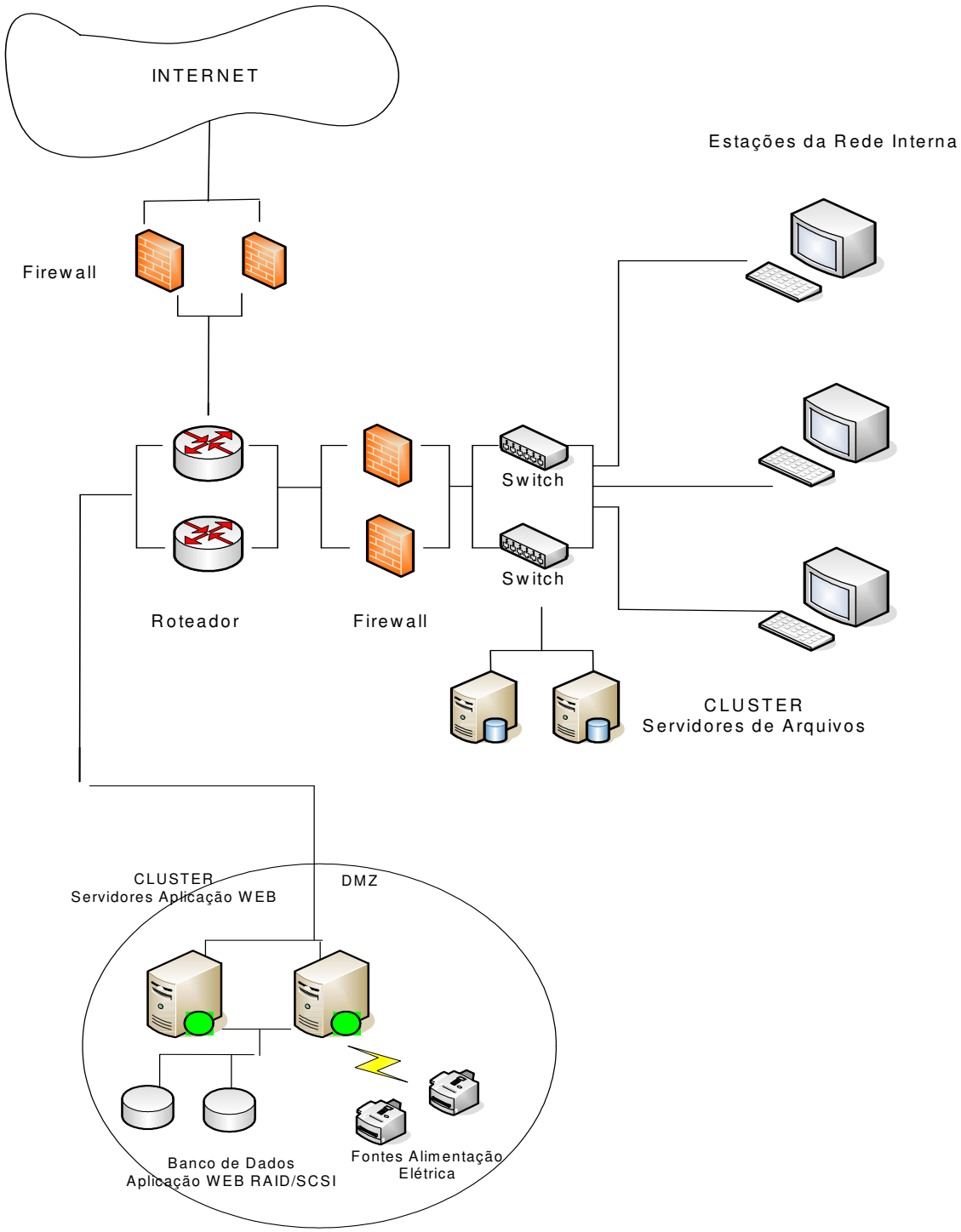


Figura 11 : Exemplo de Seção de Rede com recursos redundantes

Quadro 8 : Planilha de Prioridades de *SPOF* – Concluída

ID	Componente	Disponibilidade	Riscos	Prioridade
001CPD-001	Roteador CISCO 2500	99,17 %	Perda disponibilidade conexão Internet e Serv. *WEB*	04
003RHU-001	Switch D-link	95,36 %	Completa perda conexão das ET e Serv. Arquivos	01
001CPD-002	Firewall porta Roteador eth 0 statefull	96,98 %	Perda de filtro de saída e entrada de pacotes de Internet	11
001CPD-003	Firewall porta Roteador se 0 statefull	96,03 %	Perda de filtro de saída e entrada de pacotes rede interna	12
001CPD-004	Servidor *WEB*	95,04 %	Perda de Serviço atendimento *WEB*	07
001CPD-005	Banco de Dados aplicação *WEB*	96,76 %	Perda de disponibilidade de sistemas *WEB*	10
001CPD-006	Link Roteador-Internet	97,54 %	Perda de disponibilidade de conexão Internet	06
001CPD-007	Link Roteador-Servidor *WEB*	98,05 %	Perda conexão todo serviço *WEB*	08
001CPD-008	Link Roteador-Switch	97,99 %	Perda acesso das ET para servidor *WEB* e Internet	05
001CPD-009	Link Switch –Servidor Arquivos	97,00 %	Perda de acesso aos Sistemas Corporativos	03
001CPD-010	Fonte Alimentação Servidor *WEB*	98,23 %	Perda de disponibilidade do serviço *WEB*	09
001CPD-011	Servidor Arquivos	98,43 %	Perda de disponibilidade dos Sistemas Corporativos	02

ID	Linhas de Ação	Execução/Testes	Custos	Prioridade
001CPD-001	1- Aquisição novo roteador CISCO e implementação do HSRP	EA; atende e elimina falhas de *first-hop*	R$8.500,00	04
	2- Aquisição novo roteador e implementação do VRRP	Não aceitável, gera inoperância	XXX	
	3- Implementação de roteamento alternativo por PC	Não exeqüível, erro fatal no *firewall*	XXX	
003RHU-001	1-Aquisição de nova *switch* e implementação de *spanning tree*	EA; viabilizou caminhos alternativos	R$2.600,00	02
001CPD-002	1- Criação de *cluster de firewall* utilizando CARP e PFSYNC	EA; bem sucedido s/ perda conexão	R$ 100,00	11
001CPD-003	1- Criação de *cluster de firewall* utilizando CARP e PFSYNC	EA; bem sucedido s/ perda conexão	R$ 100,00	11
001CPD-004	1- Duplicação de Serv. *WEB* com endereço IP comum e SLB	EA; aprovado servidor criado com SLB	R$12.000,00	07
	2- Duplicação de Serv. *WEB CLUSTER HA e LOAD BALANCE*	Exeqüível e NÃO Aceitável; alto custo	R$16.000,00	12
001CPD-005	1- Implementação de RAID 5 ou 1 com discos SCSI	EA; não há outra alternativa até então	R$6.000,00	10
001CPD-006	1-Implementação de *links* paralelos com *Spanning Tree*	EA; links estabelecidos com consistência	R$250,00	06
001CPD-007			R$250,00	08
001CPD-008			R$250,00	05
001CPD-009			R$250,00	03
001CPD-0010	1- Aquisição de No Break e fontes redundantes UPS	EA; apesar do custo deve ser aplicada	R$2.500,00	09
	2- Implementação de fontes redundantes UPS	EA; inseguro na falta de energia elétrica	R$950,00	13
001CPD-0011	1- Duplicação de Serv. de Arquivos *CLUSTER HA e SLB*	EA; implementada satisfatoriamente	R$15.000,00	01

6 CONCLUSÃO

Parece razoável afirmar que, no mercado atual, a tolerância a falhas numa estrutura de redes é praticamente zero. Muitas destas falhas são previsivelmente provocadas por degradação operativa ou total inoperância de componentes da instalação. Diante do Referencial Teórico apresentado neste trabalho, pode-se afirmar que um administrador possui, como alternativa técnica para atender a grande demanda de serviços ininterruptos, a aplicação do conceito prático de redundância. Dentro deste importante recurso são disponibilizadas inúmeras tecnologias que viabilizam a eliminação dos pontos de falhas e consequentemente uma melhor oferta de serviços. Esta oferta se torna prioritária quando sistemas críticos dependem fundamentalmente da rede de dados em produção.

6.1 CONTRIBUIÇÃO

Na tentativa de estabelecer uma contribuição relevante sobre o acima exposto, este trabalho sugere que haja um compromisso com o planejamento e a adequação das soluções adotadas em busca da alta disponibilidade e da máxima confiabilidade da rede. A alternativa de elaboração da Planilha de Prioridades de SPOF (*Single Point of Failure*) (PPS) aqui apresentada, visa exatamente prestar apoio à decisão de sobre quais pontos sujeitos a falhas representam maiores riscos para a instalação, como podem ser eliminados e quais são os custos envolvidos. Desta forma pode-se estabelecer que os pontos sensíveis recebam tratamento prioritário, em prazos coerentes e com orçamentos justificáveis.

6.2 LIMITAÇÕES DA PESQUISA

As limitações desta pesquisa passam a existir no momento em que, apesar da comprovada possibilidade prática de elaboração da planilha sugerida, é razoável que existam dificuldades em relação ao preenchimento do campo Execução/Testes devido à complexidade de se gerar simulações. Desta forma, faz-se necessária a implementação da PPS em ambiente real, a fim de observar se seria alcançado o efeito desejado.

6.3 TRABALHOS FUTUROS

Como trabalhos futuros, são considerados de efetivo interesse: a implementação da PPS em ambiente real, uma maior avaliação de aplicabilidade, o aperfeiçoamento de seus campos, além da possibilidade futura de automação de seu preenchimento. O Relatório Complementar também deve receber maior apreciação quanto ao seu formato e ao modo de referenciar os dados da PPS.

REFERÊNCIAS

1- TANENBAUM, A. S. Redes de computadores. Rio de Janeiro : Campus, 1997.

2- SOARES, L. F. G. et al. Redes de Computadores: das LANs, MANs e WANs às Redes ATM - Rio de Janeiro : Campus, 1995.

3- COMER, Douglas E. - Interligação de redes com TCP-IP – Vol.1 5ª Ed Ed. Campus – 2006.

4- KUROSE, J.F. Redes de Computadores e a Internet, 3ª Ed.- Pearson Addison Wesley – 2006.

5- LOPES, Raquel – Melhores Práticas Para Gerência de Redes de Computadores, 1ª Ed. – Elsevier Editora LTDA – 2003.

6- JÚNIOR - José Helvécio Teixeira - Redes de Computadores (Serviços Administração e Segurança), 1ªEd. – Pearson Education do Brasil LTDA. – 1999.

7- AZEVEDO, Moacyr H. Cruz - Notas de aula – Projetos de Redes: Equipamentos e Infra-Estrutura – NCE – MOT/2006-2007.

8- AGUIAR Paulo – QoS em Redes – NCE – MOT/2006-2007.GONÇALVES, Luís Rodrigo de Oliveira – APOSTILA DE TECNOLOGIA DE REDES DE COMPUTADORES – 23 de março de 2006 – acessada em 13 de agosto de 2007, por: http://www.lrodrigo.cjb.net.

Páginas da *WEB* visitadas de maior importância :

9- http://pt.wikipedia.org/wiki/Redundância acessada em 10/06/07;

10- http://pt.wikipedia.org/wiki/Disponibilidade acessada em 15/06/07;

11-http://pt.wikipedia.org/wiki/Confiabilidade acessada em 18/06/07;

12-http:/www.minerva.ufrj.br - http://fenix2.ufrj.br:8991 acessada em 21/06/07.

13–http://www.clubedohardware.com.br/artigos/153 acessada em 02/07/07;

14-http://www.clubedohardware.com.br/artigos/153/2 acessada em 02/07/07;

15-www.cisco.com/en/US/docs/routers/access/3700/hardware/notes/3725rps.html#wp40257 acessada em 03/07/07;

16-http://www.cisco.com/web/BR/index.html acessada em 04/07/07.